govtech review

LEADERS IN TECH

2022 PREDICTIONS

Q4 2021
PP100021607

HOLDS UP
EQUIPMENT
NOT PROJECTS

Q4 2021

INSIDE

FEATURES

LEADERS IN TECHNOLOGY

Insider

This time last year, many of us thought that the worst of the pandemic was over and that Australia had largely escaped the turmoil endured in other parts of the world. Our relief turned out to be a little premature, as 2021 delivered more of the same... on a somewhat larger scale and for a far longer period in many metropolitan and regional areas across the country.

At the risk of once again pre-emptively breathing a sigh of relief, at the time of writing, vaccination rates around the nation are progressively reaching thresholds deemed sufficient to trigger relaxation of lockdowns, limits and other restrictions. Here's hoping it really does signal a return to something that more closely resembles life as we once knew it.

As we wrap up 2021 and start sailing into a new year, we've asked tech industry leaders to share their thoughts — not only on the operational and workplace changes brought about by two years of living in a pandemic, but additionally what those shifts will mean in a more permanent way. Are they actively shaping the likely tech pain points that government and enterprise will face in the year ahead? Will they lead to greater rationalisation and a need for more improved organisational efficiency? How will the changed landscape impact leadership, culture and 'who is in charge of what' through the next year and beyond?

One thing is abundantly clear — the pandemic has hastened digital transformation for many agencies and organisations, which presents opportunity for 2022 to move beyond building a business case or implementing pilot studies and into development of the solid framework required to support completion of that goal and deliver on expectations.

From an industry perspective, that acceleration must continue, with adoption of newer technologies like artificial intelligence and automation taken up by government and used to facilitate data-driven decisions that will improve customer interaction and service delivery — in ways that citizens have increasingly come to expect.

Whatever the year ahead holds, as we close out 2021, I'd like to wish you the best for the holiday season and hope that you and yours stay safe and well.

I look forward to returning in 2022 to bring you all the latest in technology news.

Dannielle Furness, Editor
editor@govtechreview.com.au

wfmedia
connecting industry

A.B.N. 22 152 305 336
www.wfmedia.com.au
Head Office:
Locked Bag 2226
North Ryde BC NSW 1670
Ph +61 2 9487 2700

EDITOR
Dannielle Furness

dfurness@wfmedia.com.au

PUBLISHING DIRECTOR/MD
Geoff Hird

ART DIRECTOR/PRODUCTION MANAGER
Julie Wright

ART/PRODUCTION
Colleen Sam, Krystyna Kappel

CIRCULATION
Dianna Alberry, Sue Lavery
circulation@wfmedia.com.au

COPY CONTROL
Mitchie Mullins
copy@wfmedia.com.au

ADVERTISING SALES
Liz Wilson Ph 0403 528 558
lwilson@wfmedia.com.au

If you have any queries regarding our privacy policy please email privacy@wfmedia.com.au

All material published in this magazine is published in good faith and every care is taken to accurately relay information provided to us. Readers are advised by the publishers to ensure that all necessary safety devices and precautions are installed and safe working procedures adopted before the use of any equipment found or purchased through the information we provide. Further, all performance criteria was provided by the representative company concerned and any dispute should be referred to them. Information indicating that products are made in Australia or New Zealand is supplied by the source company. Westwick-Farrow Pty Ltd does not quantify the amount of local content or the accuracy of the statement made by the source.

Printed and bound by Dynamite Printing
PP 100021607 • ISSN 1838-4307

Smarter technology for all

Lenovo

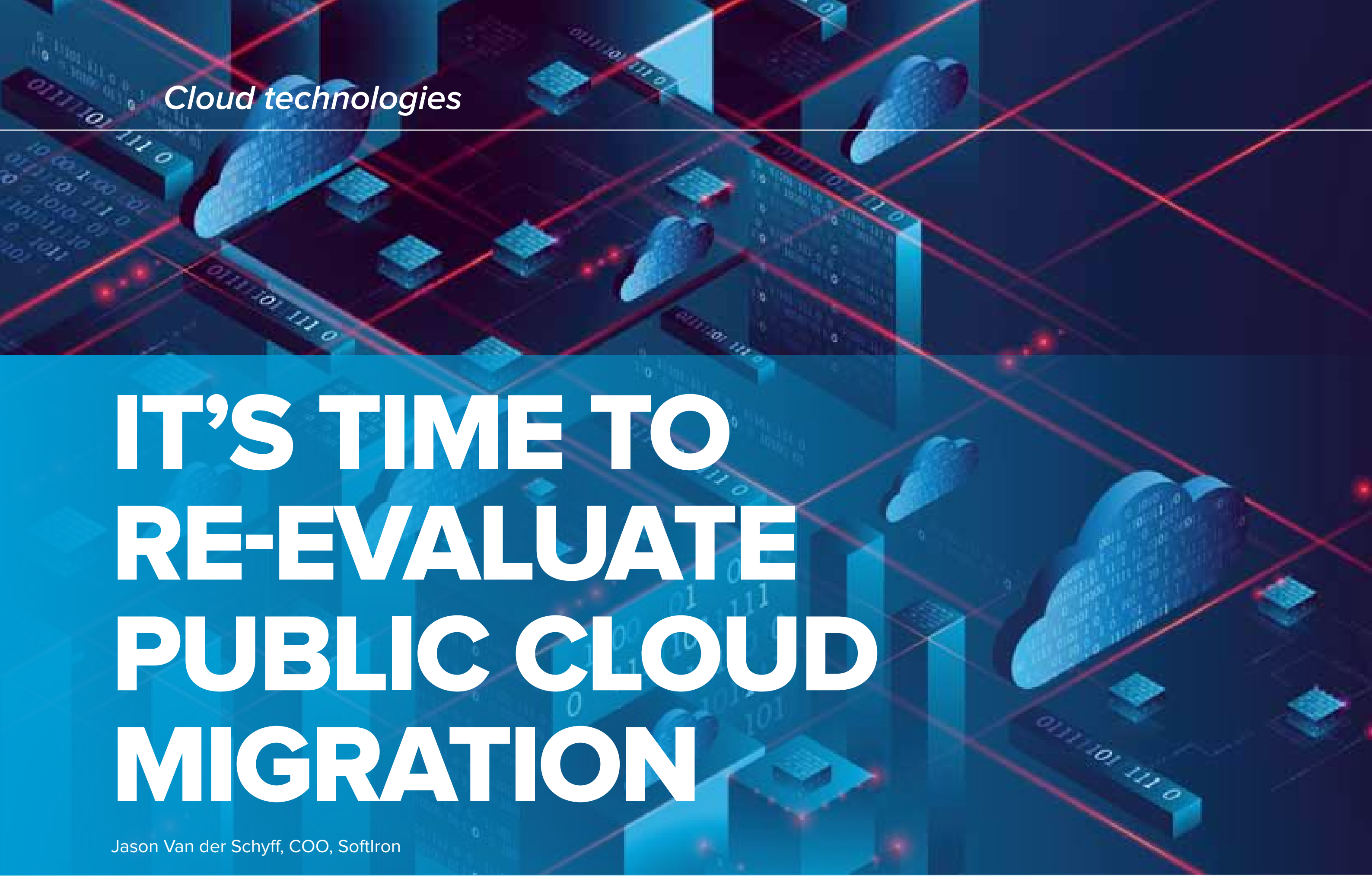
You don’t have to be together to work smarter together.

Simpler, safer, and more reliable collaboration. Our ThinkSmart devices are easy to manage and enable seamless teamwork...from wherever your people connect.

Learn more
techtoday.lenovo.com/smart-collaboration

Windows 11

Lenovo recommends Windows 11 Pro for Business



IT'S TIME TO RE-EVALUATE PUBLIC CLOUD MIGRATION

Jason Van der Schyff, COO, SoftIron

The proposed Hosting Certification Framework introduced by the Digital Transformation Agency earlier this year is a call for a new approach to building critical national infrastructure.

The framework stipulates that all relevant government data will need to be stored only in either 'certified assured' or 'certified strategic' data centres. This new approach follows concerns about the acute data challenges confronting the Australian public sector and aims to mitigate against data centre ownership risks, including data sovereignty, supply-chain vulnerabilities and cybersecurity threats.

This is a very timely addition to the regulatory framework for Australia at a time when nations around the world are responding to the challenge of building sovereign resilience. At a hosting level at least it provides the framework for better auditing and assurance of those facilities and their operation.

However, there's an issue. Are we shutting the cabinet door after the data has already bolted? What about all the data and services that have already left the infrastructure and facilities run by our public servants and are now run in the public cloud?

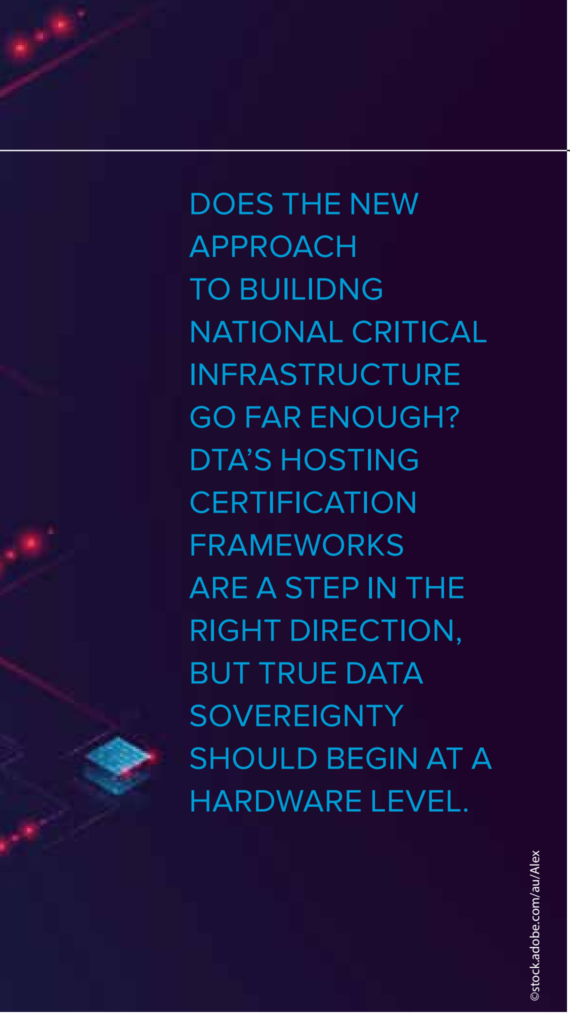
THE SCRAMBLE TO THE CLOUD IN THE PANDEMIC

Migration to the public cloud in both the public and the private sectors has been happening over perhaps a decade or more now, but has only been accelerated in the last 18 months as organisations rushed to the cloud to maintain operations during the pandemic.

However, organisations are now left figuring out how to adequately protect both data and services that are hosted in the cloud. Cloud services are essentially akin to 'someone else's computer', with many hidden behind a wall, meaning organisations who are using cloud services have little to no real visibility on how the infrastructure is really and instead must rely on 'trust'.

Time to take a breath and review where we are. The way in which organisations, particularly the Australian public sector, store and manage data now has the opportunity to change for the better. It's important for government agencies to understand the four key areas of concern for cloud services and how to overcome these challenges as they look to benefit from the new hosting framework.

And, to identify the best pathways towards sovereign resilience we first need to understand the recent drivers of the mass move to the public cloud, and the common underlying issues in the infrastructure being used to provide public cloud services.



DOES THE NEW APPROACH TO BUILIDNG NATIONAL CRITICAL INFRASTRUCTURE GO FAR ENOUGH? DTA'S HOSTING CERTIFICATION FRAMEWORKS ARE A STEP IN THE RIGHT DIRECTION, BUT TRUE DATA SOVEREIGNTY SHOULD BEGIN AT A HARDWARE LEVEL.

©stock.adobe.com/au/Alex

SO MANY EGGS, SO FEW BASKETS

The benefits of the public cloud are clear: reduced management and maintenance overhead, pay-as-you-go provisioning of popular software tools and platforms, and access to the resilience and availability a large-scale provider can offer, to name a few. But those benefits don't come without their fair share of risks; by outsourcing such a large volume of data and services to such a small number of providers, the nation's financial stability is at risk.

ACCELERATED PUBLIC CLOUD ADOPTION — THE RESPONSE TO A WORLD IN LOCKDOWN

The COVID-19 pandemic has understandably been a massive driver of public cloud adoption in recent years, bringing about a dramatic shift in how and where data is created, processed and stored. This has presented ICT teams in both the public and private sectors with considerable challenges, as entire workforces switched to remote work near-overnight.

For those organisations previously based entirely around on-premises operational models, this was a major shift, and few had the onsite infrastructure or support network to handle the sudden demand for cloud services.

The public cloud is at its best and most useful in such scenarios — providing a scalable and elastic buffer of computing power, delivering services on-demand, where and when required, while handling peaks and troughs with ease.

It's no surprise then that across many sectors, particularly the government, the transition to the cloud has been swift. There can be no doubt that access to public cloud services is now a critical tool in every industry.

'JUST SOMEONE ELSE'S COMPUTER'

As organisations are adjusting to the new way of working, the complexity of the public cloud and the risks this poses, are becoming more apparent. Cloud services are sometimes referred to as 'just someone else's computer', and this captures the core risks of the public cloud entirely.

Public cloud vendors will assert that in not disclosing information they are, in fact, doing you a service, as vectors of attack are obscured. This provides little assurance for regulators and others with vested interests in securing business and economic continuity should downtime occur or, worse, complete loss of data or services in the event of an attack.

COMPROMISED SYSTEMS CANNOT BE SAVED FROM SECURITY CONTROLS

The industry today takes a largely 'information-centric' approach to security. That is, assume that every system is compromised. Although not all systems are compromised and controls can generally only be applied to hardware systems that have already booted up and loaded their operating systems.

This leaves a window of opportunity for bad actors to infiltrate hardware and execute attacks that alter normal operations during the bootup process before the usual controls can be applied. This can lead to disrupted operations, monitoring of sensitive information, stolen or corrupted data, or even instances where complete control over a system can be taken.

To overcome these challenges, organisations need to achieve true data sovereignty, which needs to begin at a hardware level. The only way to ensure each and every component on the circuit board is doing its correct assigned task is through hardware that is transparent and auditable through Secure Provenance.

Secure Provenance ensures that the appliance is true, that it is precisely as designed and specified, with no hidden code or additional components. Achieving this means organisations can have a 360° transparent view into the entire design, supply chain, manufacture and delivery path of data centre appliances.

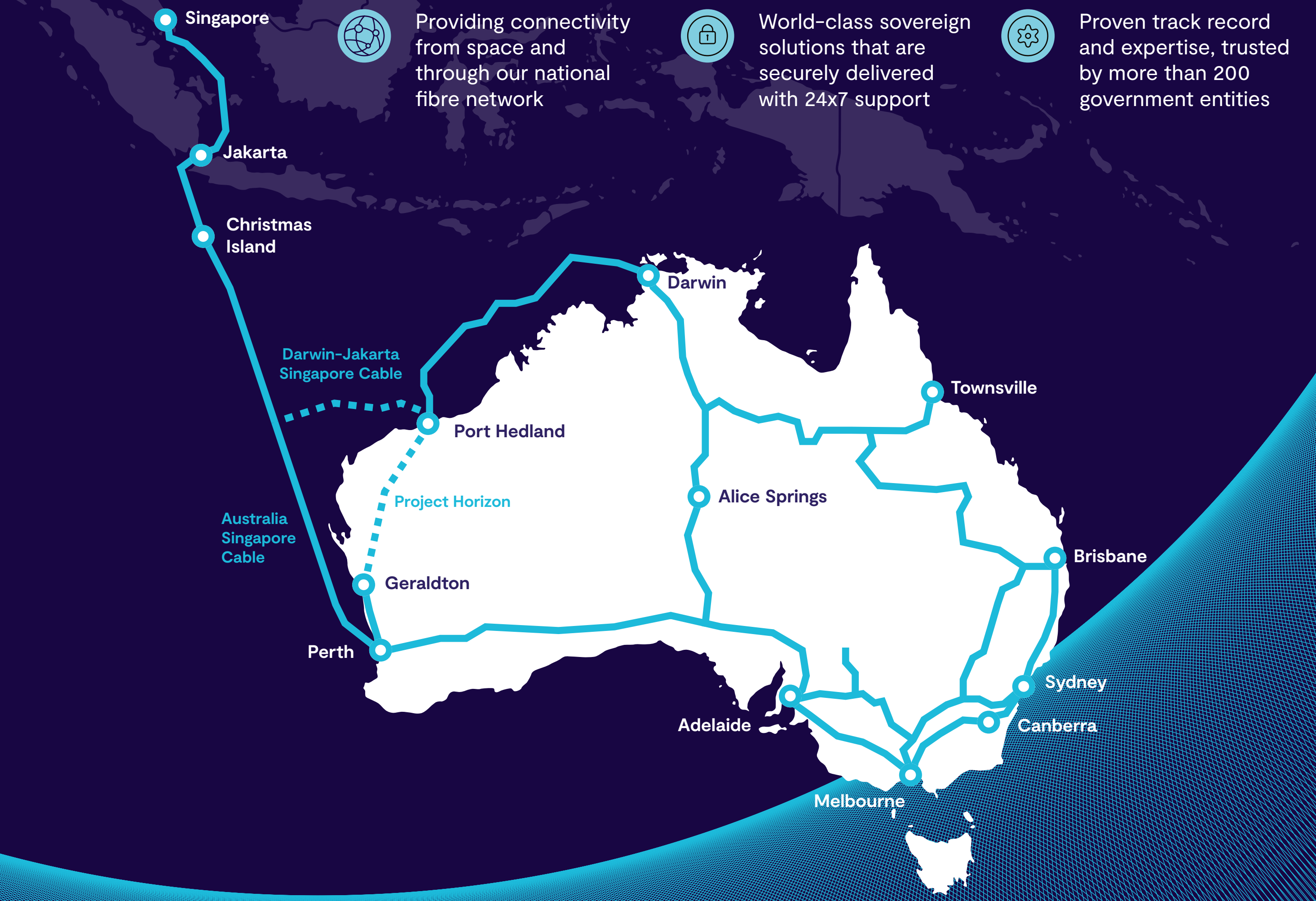
While cloud services offered organisations a scalable solution to maintain business continuity at the beginning of the pandemic, the lack of visibility and transparency means Australian data is at risk. Instead of hosting data on someone else's computer, organisations need to strive for Secure Provenance.

The Hosting Certification Frameworks proposed by the DTA are a step in the right direction to mitigate against data centre ownership risks. However, true data sovereignty needs to begin with hardware that is hosted within that framework to ensure that it is true, transparent and completely auditable.

Australia's specialist fibre and network solutions provider

We're a critical infrastructure provider and play a key role in helping to securely deliver government services to Australian people, businesses, and communities in cities, towns, and remote areas.

- Providing connectivity from space and through our national fibre network
- World-class sovereign solutions that are securely delivered with 24x7 support
- Proven track record and expertise, trusted by more than 200 government entities



We make it simple for governments to go forward, go further and grow faster.

Contact us on 1300 88 99 88
or visit vocus.com.au/government

VOCUS
Brilliant made simple

KEVIN GRIFFEN

GM ENTERPRISE SALES — ENTERPRISE & GOVERNMENT, VOCUS

LEADERS IN TECHNOLOGY 2022

HOW HAS AUSTRALIA COPED WITH COVID-INDUCED CHANGES TO OPERATIONS AND WORKPLACES? WILL THINGS GO BACK TO A 'NEW NORMAL' IN 2022?

Full-time work from home was not in anyone's plan. Before the pandemic, it was impossible to think that such a widespread shift would've occurred — in fact, most businesses probably wouldn't have wanted it to happen. The situation forced everyone's hand and accelerated the future of work in a way that no-one thought possible. Changes that would have taken years to implement happened in a matter of days. A 'new normal' is evolving, combining the wants and needs of employees, employers, businesses and governments in a balance that has not been seen before.

Much of that was positive: businesses are now more flexible and agile than ever before. Engagement and operations have been digitised, and employee health and wellbeing are at the forefront. But, as organisations adapt to the reality that flexible work isn't going away, they are taking a more strategic approach to enabling technologies. Tech decisions that were made hastily during COVID and new tech needs that are arising are all being evaluated to determine the big question: does it do what we need and want it to do?

WHICH NEW TECHNOLOGIES WILL REACH CRITICAL MASS AND BECOME DOMINANT IN 2022?

The future of work is here now, and technologies that enable that for employees and end customers should be the focus for organisations in 2022. That includes connectivity, including fibre networks and satellite options, to ensure that people in hard-to-reach places have reliable, cost-effective options.

Distributed cloud is quickly becoming a requirement for many businesses that require their tech to be closer to where their people and services are. Network latency goes hand in hand with distributed cloud, enabling technology like low earth orbit satellites. Hyper automation, or streamlining business processes using people-free tools, is also proliferating. It allows businesses to align their processes quickly and efficiently to their needs.

WHAT IS THE MAJOR POTENTIAL TECH PAIN POINT THAT WILL FACE ALL ORGANISATIONS LARGE AND SMALL IN 2022?

Businesses had to quickly pivot during COVID to enable employees and deliver for their customers. With the immediate threat behind us, organisations are now assessing what those decisions have meant, and what should be done going forward. With people working in disparate locations, security and risk management are topics of concern, and businesses of all sizes should be taking steps to ensure that no matter where an employee is working from, data and systems are protected.

But to do all that, security personnel are required and businesses in every industry are struggling to get enough skilled staff. Programs or technology aren't the pain point, but the lack of staff to run these things is, and will continue to be, for organisations of all sizes in 2022 while we all adjust to our post-pandemic reality.

HOW CAN I.T. HAVE A GREATER IMPACT ON ORGANISATIONAL EFFICIENCY IN 2022, AND WHO (CEOs, CIOs) SHOULD LEAD THE CHARGE?

The problem organisations will see in 2022 isn't a lack of organisation efficiency but getting staff to collaborate and work efficiently together. It's a slight difference but a big one — the former is a technology problem, while the latter is a cultural issue.

Instead, the focus will be on readjusting to new business cultural norms going forward. Maximising people's belief in what they do, bringing the culture of an organisation to wherever people are working from and maintaining team cohesiveness — it's not one department's job, but rather a business-wide decision of how the organisation will operate and create a consistent employee experience going forward. This is paramount: if your staff are culturally misaligned or don't feel like they are contributing to a greater mission, then no amount of technology or high-tech gadgets will help.

Kevin is the GM Enterprise Sales, Enterprise & Government, at Vocus. He's enjoyed a 30-year career in the ICT industry encompassing corporate leadership, sales management and business development with some of Australasia's largest companies. His guiding philosophy is that people are a company's greatest asset from which all success flows.

SCOTT HESFORD

DIRECTOR OF SOLUTIONS ENGINEERING, APJ, BEYONDTRUST

LEADERS IN TECHNOLOGY 2022

HOW HAS AUSTRALIA COPED WITH COVID-INDUCED CHANGES TO OPERATIONS AND WORKPLACES? WILL THINGS GO BACK TO A 'NEW NORMAL' IN 2022?

In 2021, the pandemic remained with us. While cyberattackers had exploited the pandemic during its earliest stages, late 2020 through 2021 was when the abundant attack surfaces created by rushed implementation of remote working and digital transformation initiatives began to be exploited with vigour. Cybercrime exploded. Once-in-a-decade breaches (SolarWinds, Colonial Pipeline, Nine Entertainment, JBS foods, Kaseya) seemed to occur monthly. The proliferation of cyberthreats, breaches and the accelerated de-perimeterisation of enterprises also catapulted the concept of zero trust from security aspiration to a security mandate.

During these last two years, our collective digital dependency has only increased. The stakes for protecting digital assets and critical infrastructure from cyberattacks is only getting more urgent, while ever-more difficult to achieve. There is no turning back.

WHICH NEW TECHNOLOGIES WILL REACH CRITICAL MASS AND BECOME DOMINANT IN 2022?

Today, IoT technology is pervasive and is appearing in parts of the enterprise that would have been unfathomable just a few years back. Consumers and businesses can expect that newer devices will be cellular-enabled, or cellular-capable, to provide services outside of local area and Wi-Fi networks. This will allow connectivity using a subscription model and remove the barriers and troubleshooting required for connectivity on home or small business networks.

Continuous connectivity, regardless of environmental conditions, will be highly appealing to most users — especially for security-related systems like alarm systems and cameras.

WHAT IS THE MAJOR POTENTIAL TECH PAIN POINT THAT WILL FACE ALL ORGANISATIONS LARGE AND SMALL IN 2022?

Record-breaking ransomware payouts in 2021, including $40 million paid by one victim's insurance company, continued to validate the ROI and economics of ransomware for threat actors.

This year, the ransomware model evolved to include data extortion based on exfiltrated information. But ransomware is not done evolving. New paradigms to extort money will emerge in 2022.

Organisations should expect ransomware to become personalised and increasingly involve different types of assets, like IoT, as well as company insiders. Targeted disclosure of exfiltrated information may be perpetrated to specific buyers. We may even start to see more flexible terms of payment, as opposed to lump sum payouts. With instalment plans, ransomware operators will decrypt victim assets over time, based on agreed upon payout terms.

WHAT'S ON YOUR TECH WISH LIST FROM GOVERNMENTS, INNOVATORS AND THE WIDER INDUSTRY IN 2022?

Since the advent of networking, the attack chain has typically comprised such steps as exploitation of a vulnerability, obtaining of privileged access, lateral movement, and exfiltration of data or operational damage. Each year, it's hoped that next year will be the year we get the basics right and the number of successful attacks declines.

In 2022, the number of successful attacks will most likely continue to grow, the average cost to the victim organisation per successful attack will rise and the pattern will repeat. Why? Because with so many new and shiny technologies to choose from, the IT security basics just aren't exciting. It would be good to be wrong on this one and see the industry break this chain.

Scott Hesford has over a decade of experience in cybersecurity. Before joining BeyondTrust in 2019, he worked as Principal Consultant for CA Technologies. A trusted cybersecurity advisor to enterprise customers, his experience spans several industries including banking, insurance, energy and utilities, in addition to state and federal governments.

FLYING HIGH

IN OUR ANNUAL LEADERS IN TECHNOLOGY SERIES, WE ASK THE EXPERTS WHAT THE YEAR AHEAD HOLDS. WE TALK DRONE TECHNOLOGY WITH HOVER UAV'S JACKIE DUJMOVIC.

When Jackie Dujmovic was first introduced to drones, she saw boundless potential. She was so convinced of the promise presented by the then emerging technology, she immediately acquired her UAV licence and founded Hover UAV to further explore the possibilities.

Jackie's maritime background meant her initial interest leaned to conservation applications, which led to development of a world first — a shark alarm that could be attached to an uncrewed aerial vehicle and help save lives. That same pioneering spirit is still what drives the Hover UAV team. Focused firmly on the future and always a step ahead of the curve, the company is a preferred provider in both the private and public sectors, conducting major drone operations across a range of industries and applications.

We spoke with Jackie about life in a post-pandemic world and what 2022 holds for industry and government when it comes to the use of UAVs.

"While the pandemic presented a few logistical challenges in terms of border closures and other restrictions, it didn't fundamentally change the way our business operates, because much of what we do is remote.

"Generally, of course, it did create a renewed focus on the future, especially looking at how people will work. When it comes to drones, we are seeing huge interest in moving away from the traditional 'visual line of sight' control, where the pilot is onsite, towards highly automated operation — or 'drone in a box'.

"That's absolutely where our technology and our offering is headed. We're in the process of developing a remote operation centre to facilitate this," she said.

2022 will be a year of reckoning for many organisations, according to Jackie, with one of the greatest challenges being delivery of efficient drone programs.

"The use of drone technology is increasingly attractive for government departments and other industry sectors because there is so much that can be done more effectively and efficiently.

"While many organisations have identified use cases and carried out proven trials, they now need to move beyond that point, and they need to do it safely. This can be a real challenge when aviation is not the core function of your business or agency.

"Regardless of whether the required capability exists in-house or is pulled from an external resource, successful deployment requires clearly defined internal policies and appropriate structures be in place, including a solid digital framework from which to build," she said.

Ensuring the right people are involved is essential, as is having a clearly defined outcome.

"The CIO is key to the process. While drones are useful for gathering data, success in UAV programs means being clear about what type of data is needed and how it will ultimately be used. This clarity must be there from the outset and the CIO will help define that," she said.

For agencies hoping to build solid programs around UAV technology, understanding the regulatory requirement and ensuring compliance is a huge part of the undertaking.

"The regulations do change, and that can be a significant challenge if there is a lack of embedded aviation experience. Our position is to support organisations in their individual journeys and to ensure compliance. It's all part of having a good foundation in place that will enable those agencies to grow and enable them to push to the next level," she said.

Hover UAV founder and CEO Jackie Dujmovic is a recognised industry innovator and commercial drone pioneer. She will present 'Drones for mission-critical response' at the Comms Connect conference being held in Melbourne in March 2022.

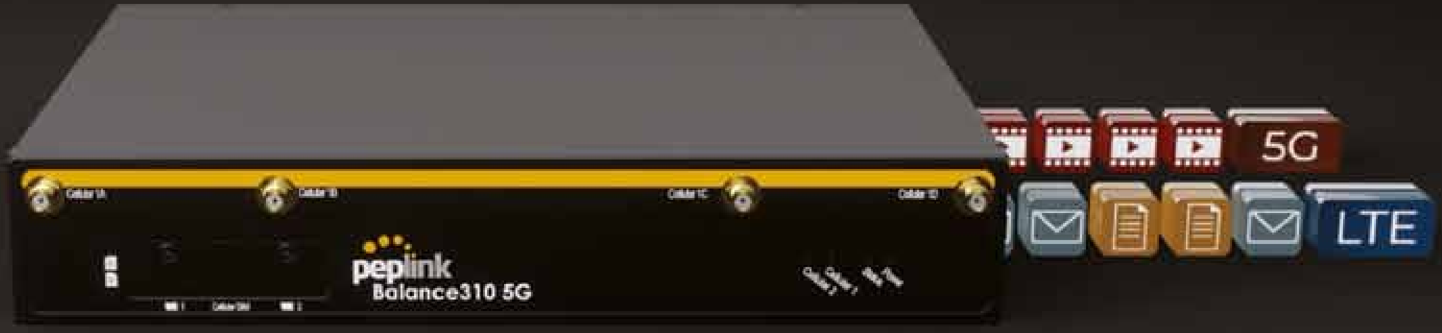
B310 5G

WirelessTech

5G-Hybrid Enterprise Branch Connectivity

Balance Your Fixed Network with 5G Wireless WAN

With SpeedFusion Cloud you can utilise traffic steering. A technology whereby connections are controlled based on the application, limiting data wastage and traffic.



Enjoy Speed and Reliability without Having to Compromise

Multi-radio combined with our SpeedFusion Hot Failover technology allows connections of 5G and LTE networks to work simultaneously.

InControl²

Control Anytime Anywhere

Remote Central Management with private controller or cloud management.

WirelessTech

+61 2 8741 5080 | sales@wirelesstech.com.au | www.wirelesstech.com.au

©stock.adobe.com/au/zephyr_p

Ransomware Action Plan: what comes next?

Alison O'Hare

Ransomware has been a concern for IT leaders for several years but has escalated in recent years, and the recent announcement of the Australian Government's Ransomware Action Plan (RAP) reinforces the seriousness of the problem.

Mimecast closely tracks cybersecurity trends year-on-year, and we're seeing an annual increase in ransomware attacks. Mimecast's State of Email Security (SOES) Report 2021 revealed that six out of 10 Australian organisations suffered a ransomware attack last year, which is a significant rise from 48 per cent the previous year.

Until now it's been unclear whether companies should or shouldn't pay ransoms, with no streamlined guidance. Now, the Government has clearly stated in the RAP that it does not condone the payment of ransoms.

The SOES report found that, out of the 54 per cent of Australian businesses that paid a ransom, 24 per cent did not recover their data, even after paying up — highlighting that paying a ransom is not the best option and further validating the government's stance.

That said, according to Mimecast's inaugural State of Ransomware Readiness Report 2021, over half of Australian executives (55 per cent) feel they could lose their job as a result of a ransomware attack.

This means that huge focus needs to be given to how to effectively implement mandatory reporting of attacks. Consideration to the reporting of attacks must ensure that the problem isn't pushed underground by executives, nervous that their careers could be on the line if they report and shine a spotlight on their organisation's ransomware woes. Close collaboration with the cybersecurity industry will be essential when working through the details.

What's next for SMB IT leaders?

Mandatory reporting of attacks is only being proposed for businesses turning over $10 million or more per year. The RAP in its current form will therefore not go anywhere near measuring the true scope of the problem, when you consider that businesses which fall below the proposed reporting threshold account for 98 per cent of Australian businesses, according to ABS data.

SMBs have not been completely isolated from the Ransomware Action Plan, with reference to some support being offered to these organisations. However, at Mimecast we strongly believe there needs to be a level of 'cybercare' available for SMBs, just like healthcare for citizens.

According to the State of Ransomware Readiness Report, nearly half of Australian executives would also like additional resources for more frequent security awareness training of end-users (40 per cent) and up-to-date security systems (38 per cent). Many of these executives are from larger organisations and with smaller companies even more limited on budget and time, it's natural to conclude they would benefit even more from additional support. Like universal healthcare, Cybercare holds economic benefits for the community by providing strong, streamlined, cybersecurity protection at an individual and business level, making it a valuable investment in the growth of our economy.

It also helps harden the thousands of supply chains that SMBs are involved in, which is immeasurable in its value.

While we look forward to consulting with the public sector on the details of the Ransomware Action Plan, we encourage IT leaders across private and public sector to stay up to date with the latest government/industry recommendations.

Learn how to fight back against ransomware at www.mimecast.com/anz/ransomware.

mimecast

Mimecast
www.mimecast.com

Unified security, unlimited possibilities.

Securing your organization requires more than video surveillance. To be successful, you need access control, intercom, analytics, and other systems too. This is why our Security Center platform excels. It delivers a cohesive operating picture through modules that were built as one system. So, whether you're securing an airport, a parking structure, a multi-site enterprise, public transit, or an entire city, you can access all the information you need in one place.

Genetec™

To learn about the benefits of unifying your security operations visit
genetec.com

Genetec™
Security Center.

GEORGE MOAWAD

COUNTRY MANAGER ANZ, GENETEC

LEADERS IN TECHNOLOGY 2022

HOW HAS AUSTRALIA COPED WITH COVID-INDUCED CHANGES TO OPERATIONS AND WORKPLACES?

It's been amazing to see how organisations have leveraged the power of science and technology to navigate many of the challenges COVID-19 posed, both in the security industry and across wider business and public sector organisations — most notably the medical industry. In fact, many of the innovative solutions Genetec created to help organisations navigate new business practices and regulatory requirements came from a direct collaboration between our customers and our developers. Customers told us the problem that they needed to solve and then our developers were able to update existing tools so they could be put to new uses. For example, we created a new Occupancy Management Package to make it easy for retailers and other similar businesses to ensure they operate within local guidelines for occupancy density.

WILL THINGS GO BACK TO A 'NEW NORMAL' IN 2022?

From a security industry perspective, the disruption to the public and private sectors has given many organisations the impetus to take a step back and think about what their new playbook for security in the future might look like. There's a great opportunity for security to become much more aligned with business operations and transition from a necessary and separate 'defence' function to help drive operational insights, efficiencies and performance — and the time is right as many businesses are reimagining operations as hybrid and mobile ways of working are becoming normalised. Pre-pandemic we were already seeing the merging of physical and cybersecurity and this trend has been turbo-charged as cybercriminals have taken advantage of the vulnerabilities. We'll also see many more solutions addressing biological risk be added into the physical, cyber and digital risk mix.

WHAT IS THE MAJOR POTENTIAL TECH PAIN POINT THAT WILL FACE ALL ORGANISATIONS LARGE AND SMALL IN 2022?

For many organisations in 2022, the changes coming to the Critical Infrastructure Bill will cause several pain points within the sectors soon to be included in its remit. For example, if you're in the food and grocery sector, your physical and cybersecurity planning would have looked a lot different in 2020 than it does now and businesses will have to scramble to make sure they are compliant. Changes will have to be made across both technology and organisational process, which will mean significant challenges — all of them for the potential of the greater good.

HOW CAN I.T. HAVE A GREATER IMPACT ON ORGANISATIONAL EFFICIENCY IN 2022, AND WHO (CEOs, CIOs) SHOULD LEAD THE CHARGE?

From where we are standing, it's clear that technology decisions are no longer solely in the remit of traditional IT departments and CIOs as they often underpin whole-of-business operations. This is a positive move as it means organisations are moving out of a silo mentality when it comes to critical investments in technology; however, it does mean that the lifecycle for decision-making has extended as multiple conversations with multiple stakeholders have to take place. Ultimately, CEOs are going to be the gatekeepers and enablers of organisational efficiency but IT teams have a real opportunity to make an impact if they can move from their traditional swim lane to embrace a more agile, business-orientated approach.

George Moawad joined Genetec in May 2018 and is responsible for leading business growth and nurturing expanding market opportunities for the company in the region. He has over 22 years of experience in the security industry and holds an MBA from the Australian Institute of Business.

© Stock.Adobe.com/au/FS Productions/Blend Images

THE PANDEMIC TAUGHT US HOW TO APPROACH THE NEXT SET OF RISKS

Angela Fox, Senior Vice President and Managing Director of Dell Technologies Australia and New Zealand

The past two years were a sharp lesson on why you need to think about the unthinkable. Previously, the notion that the world could screech to a standstill due to a pandemic wasn't impossible but appeared more movie plot than reality. While, thankfully, we've been able to reclaim some of our lives, it's important that we apply the lessons we've learnt to prepare us for the risks on the horizon.

Navigating risks requires digital transformation, especially when we live in the data era. Every technology that matters today creates, consumes, enriches, processes, or exploits data. This will accelerate with the adoption of edge-based computing, 5G networks and multi-cloud environments as well as artificial intelligence and machine learning, with IDC estimating that in just four years, the data ecosystem will reach 163ZB.

To realise the benefit and manage the risk of this, businesses and government must transform how they run their businesses, provide their services and interface with their customers. Before the pandemic, the last wave of our annual Dell Technologies Digital Transformation Index survey clearly showed us that most (63 per cent) Australian and New Zealand organisations were still in the "getting around to it" phase of digital transformation.

This proved problematic once the pandemic arrived. Those already underway or leading were far better equipped to successfully respond to the changing landscape, provide services and continue operations.

GETTING AROUND TO IT NOW

The seemingly simple act of working from home was difficult from both a cultural and technology perspective and unfortunately this was especially true for government. But the silver lining is what we achieved. Many government departments, including the Australian Tax Office, Australian Bureau of Statistics and Department of Defence embraced the technology available to them, that allowed them to seamlessly continue to offer services while operating remotely.

This shift meant that paradigms that had no justification could be swept aside, setting up new ways of working for many in the public sector. Governments and their agencies can not only embrace but influence this change in the wider Australian landscape. One relatively small example of the change that the government can drive is e-invoices. Since 2020, Commonwealth agencies were committed to paying e-invoices within five days and from July next year, e-invoices are mandatory for all agencies and will be encouraged from their suppliers, a strong motivator.

And of course, the Prime Minister's Digital Transformation Taskforce seeks to ensure Australia is a leading digital economy by 2030.

THE CHANGING RISK LANDSCAPE

With so much at stake, businesses accomplished in months, what would normally have taken them years. Our research shows that 8 in 10 businesses fast-tracked at least some digital transformation programs during the pandemic. The mix of programs show that many are seeking to deal with the risks and challenges they face now but also put themselves in a better position to adapt and thrive in whatever is around the corner.

Obviously, that meant strengthening cybersecurity defences, improving working from home/remote working capabilities, and reinventing digital experience delivery for customers and employees. But it also meant using data in new ways or transforming services and consumption models.

Accelerated programs present an opportunity to both mitigate risk and create new opportunities. So as the post-pandemic world comes into sharper focus, now's the time to consider digital transformation through the lens of how we deal with the new landscape and the risks within it.

MANAGING THE COMPLIANCE CONUNDRUM

The data proliferation brings with it a need for tight governances to manage privacy, record retention, competition, and consumer rights. It's not just at a local level either. As technology erodes barriers to trade and engagement, legislation like the General Data Protection Regulation (GDPR), means any businesses with international operations touching the EU need to ensure compliance.

Not only is there more data that is subject to increased regulation, but there's the complexity of IT environments with data housed on-premises and in public, private and hybrid clouds, all needing different levels of protection. Without a unified view of the data, this gives rise to a confusing mix of data management solutions that can lead to inefficiency, as well as increased costs and risks associated with data loss.

SUPPORTING PEOPLE, NOT JUST SYSTEMS

The past 18 months have disrupted the workforce in ways as deep as the arrival of the computer or internet did. Many of us relished the flexibility of working remotely, but eventually, we started feeling the negative effects of days glued to a screen, jumping from virtual meeting to virtual meeting.

While it's clear that hybrid work practices are here to stay, we need to continue to balance drawing the best from our people through collaboration and ideation, while preserving and nurturing their physical and mental well-being.

During the pandemic, it became clear that mental health support wasn't just something nice to say in your recruitment drive, but a fundamental part of your duty of care as an employer. It's important to note that this expectation of support from team members will continue, as the pandemic led many to re-examine what they expect from their employers.

TRANSFORMATION NEEDS PEOPLE AND MACHINES

Which is a great segue into possibly the biggest risk facing employers in the private and public sector, the digital skills shortage. The latest ACS Digital Pulse Report prepared for the industry body by Deloitte estimates that 60,000 more IT workers will be needed per year over the next five years. On top of that, the cost of hiring software developers, security specialists and data experts has increased by 30 per cent over the last 12 months.

Emerging technology like artificial intelligence and machine learning means Australia requires an AI specialist workforce of between 32,000 and 161,000. IT executives now see the talent shortage as the most significant adoption barrier to 64 per cent of emerging technologies, compared with just 4 per cent in 2020, according to a new survey from Gartner.

To deal with this, together, across both the public and private sector we must work collectively to build the digital skills needed both today and into the future.

BUILDING CYBER RESILIENCE

And then there's the changing threat landscape. The pending Critical Infrastructure Bill is part of a wider conversation about how we view and respond to cyber threats. Many CISOs are focusing their investments on their ability to respond and recover, rather than continuing to focus on identify, detect and protect.

For this to happen, organisations need to modernise and harden their recovery systems to ensure trusted recovery at speed. From there it's about assessing critical data and systems to find where you need to invest and where you don't.

Thirdly, we need to drive a program of continuous improvement that includes incident response and data management. Many organisations have significant investments in cyber security tools, but could still drive more value out of them, or divert their investment into cyber resilience capabilities.

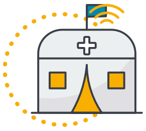
Technology is at the core of everything we do in a data centric world, and it will power our ongoing prosperity and success in Australia. This will both create risk as well as provide us with improved ways of managing that risk. Consequently, accelerating our digital transformation has never been more important as we drive a culture of continuous improvement and readiness.

Dell Technologies
www.delltechnologies.com

How Government Agencies Use LTE and 5G for Digital Transformation

Every government agency's employees need consistent and reliable access to the digital tools they use on a daily basis. Citizens are also demanding enhanced communication and services from government agencies – which rely on great connectivity. In a wide variety of situations, departments need the right network assets deployed today that can scale to meet the requirements of the future. Cradlepoint's NetCloud Service and cellular-enabled routers and adapters unlock the power of 4G LTE and 5G to securely connect federal workers no matter where their mission takes them.

SOLUTIONS Wireless Edge Routers and Adapters for Locations, Vehicles, and IoT

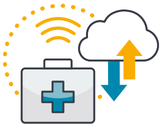


Pop-Up Networks

LTE and 5G allow government employees to quickly deploy wireless connectivity for operations including emergency services, food and safety inspections, and aircraft maintenance. Staff can easily set up connectivity in the field without reliance on another organisation's network.

Remote Work from Anywhere

Having a secure, dedicated network for high-bandwidth technologies is a necessity for government workers who work from home and abroad. Issuing Wireless WAN routers to remote staff allows IT personnel to centrally monitor and control network performance and information security.



Disaster Response Kits

Disaster response kits serve as a highly portable tool for setting up a dependable and secure network to ensure critical work can begin immediately. Hardened kits featuring ruggedised LTE routers can be used in a range of harsh environments as an integral part of emergency response.

Smart Bases

Today's military bases use IoT technologies including surveillance cameras, security equipment, and drones. Using a cellular router to connect each IoT device and/or application enables IT teams to deploy these technologies anywhere quickly, and on wireless connections that are separate from other parts of the on-site network architecture.

Mobile Command Centres

When responding to an incident, agencies need flexibility to take their operations into the field. Mounting a ruggedised, cellular- and Wi-Fi-enabled router in a mobile command centre provides the 24x7 connectivity that field agents need to work and communicate efficiently "on the move."

Smart Cities

There are many ways wireless technology can make cities run smarter, faster, and cheaper. Benefits of wireless cellular connectivity include day one connectivity and remote management, while use cases can include sensors and surveillance, and in vehicle connectivity.

Learn more at **cradlepoint.com**

Phone: (02) 8916 6334

NATHAN MCGREGOR

SENIOR VICE PRESIDENT SALES — ASIA PACIFIC, CRADLEPOINT

LEADERS IN TECHNOLOGY 2022

HOW HAS AUSTRALIA COPED WITH COVID-INDUCED CHANGES TO OPERATIONS AND WORKPLACES? WILL THINGS GO BACK TO A 'NEW NORMAL' IN 2022?

COVID-19 forced organisations to transform in real time in order to continue operations. For many, fast and easy to deploy, agile, reliable and secure Wireless WAN (WWAN) connectivity met the need to serve distributed employees and customers in new places and in new ways.

IDC's Future of Connectedness Survey[1] found that 40% of enterprises want to improve their competitive position through speed and flexibility with 5G, SD-WAN and Wi-Fi 6 over the next 12–24 months, while nearly 35% aim to invest in technology that helps connect people, things, processes and applications. Wireless WAN provides enterprises with a fast and flexible network that extends connectivity to areas wires don't easily go, or don't go at all, enabling business transformation and success.

HOW CAN I.T. HAVE A GREATER IMPACT ON ORGANISATIONAL EFFICIENCY IN 2022, AND WHO (CEOs, CIOs) SHOULD LEAD THE CHARGE?

1. Improved uptime means not only improved productivity but also increased confidence in the adoption of WWAN as primary and failover connectivity in more locations.
2. Using WWAN significantly reduces WAN operating costs: Participants in a Nemertes analysis[2] reduced staff dedicated to WAN by an average of 19%, and WAN staff spent 54% less time troubleshooting WAN issues.
3. Cloud managed WWAN solutions provide the ability to preconfigure and centrally deploy, monitor, manage, analyse and troubleshoot connectivity and security for all locations — reducing truck rolls, people-hours and costly downtime.

While CEOs might set the business transformation strategy and revise company policy as to when and where people work, CIOs will design the infrastructure that enables these changes to happen.

WHICH NEW TECHNOLOGIES WILL REACH CRITICAL MASS AND BECOME DOMINANT IN 2022?

Organisations are trialling and investing in 5G connectivity to ensure they have the best tools available to adjust to changing conditions. 5G technology is fibre-fast and cellular simple, and has proven itself as a critical enabler in customer innovations and working remotely. We expect such use cases to continue to grow.

WHAT IS THE MAJOR POTENTIAL TECH PAIN POINT THAT WILL FACE ALL ORGANISATIONS LARGE AND SMALL IN 2022?

Hybrid working is here to stay, and leaders must find a way to deliver an office experience from a reliability, security and I.T. management perspective, to a remote workforce. The key to enabling managed, secure and performant networks is deploying an I.T.-controlled router with dedicated WWAN and WLAN environments. Leveraging 'corporate-owned' 4G and 5G cellular connections offers universal and reliable WWAN connectivity to every employee's home regardless of their home internet provider.

WHAT'S ON YOUR TECH WISH LIST FROM GOVERNMENTS, INNOVATORS AND THE WIDER INDUSTRY IN 2022?

While LTE has been enabling businesses to leverage wireless and 'cut-the-cord' solutions for a while, the speed, intelligence and resiliency of next-generation 5G services is becoming a catalyst to Wireless WAN adoption. Not only does it make today's applications better, but it will also enable a new generation of immersive customer experiences at the network edge, as well as more cost-effective SD-WAN 5G architectures, anywhere connectivity and high-speed wireless failover for larger sites.

Sources:

[1] IDC, The Future of Connectedness: Technology Priorities for an Agile Enterprise, Doc #US48252821, September 2021

[2] Nemertes Business Value Analysis, The Viability of a Wireless WAN for Business, December 2020

Nathan McGregor is the Senior Vice President, Sales for the Asia Pacific (APAC) region at Cradlepoint. Nathan has over 20 years' leadership experience in the telecommunications and IT industry working for prominent companies, including Cisco Meraki, Hitachi, Juniper Networks, Ericsson and Alcatel Lucent.

CYBERARK

HELPING GOVERNMENT BRIDGE THE CYBER DIVIDE

CyberArk in association with Innovation.Aus present the 'Bridging the Cyber Divide' Podcast Series.

Episode 1:

Securing a digital economy

Robert Deakin - Director of Cyber Security, ACCC (Australian Competition and Consumer Commission) & CyberArk's ANZ Regional Director, Thomas Fikentscher discuss Australia's move towards becoming a digital economy and associated security implications.

Episode 2:

Bridging the Public/Private divide

Dr. Stephenie Andal, Head of Strategic Policy at the Cyber Security Cooperative Research Centre and Thomas Fikentscher, ANZ Regional director at CyberArk, discuss what can governments learn from the private sector.

Episode 3:

Demystifying the Price of Privilege

CyberArk's ANZ Regional Director, Thomas Fikentscher discusses improving security in 2021 - with more devices, new business models & a more diversified workforce.

Episode 4:

Street Creds

Matt Tett, Manageing Director at Enex TestLab and Andrew Slavkovic, Solutions Engineering Manager at CyberArk discuss the approach to IRAP, FedRAMP and other compliance schemes to better understand how regulatory systems have changed.

Episode 5:

Critical Connections

Lani Refiti, Co-Founder and CEO at IoTSec Australia and Jeffery Kok, VP of Solution Engineers at CyberArk discuss the rapid expansion of IoT capability and the arrival of 5G in Australia. Security remains key to underpinning successful implementation.

Episode 6:

Scaling Cyber Skills

Prof. Richard Buckland, Professor of Cyber Security at UNSW and Bruce Nixon, Partner Manager at CyberArk discuss the speed with which the cyber security landscape is changing has put constant pressure on the availability of skilled cyber professionals.

Episode 7:

Navigating Privacy and Law

Mike Trovato, Managing Director at Information Integrity Solutions and Thomas Fikentscher, Regional Director at CyberArk, discuss Navigating Privacy and Law.

Episode 8:

Security in transformation

Barak Feldman, Senior Vice President and Thomas Fikentscher, Regional Director at CyberArk discuss security in transformation with - Alastair MacGibbon Chief Strategy officer at CyberCX and former head of the Australian Cyber Security Centre and Cyber Security advisor to the Prime Minster of Australian.

THOMAS FIKENTSCHER

REGIONAL DIRECTOR ANZ, CYBERARK

LEADERS IN TECHNOLOGY 2022

HOW HAS AUSTRALIA COPED WITH COVID-INDUCED CHANGES TO OPERATIONS AND WORKPLACES?

From my vantage point working with a cross-section of Australian public and private sector organisations, businesses did an amazing job at rapidly pivoting working environments when everything changed in March 2020. Organisations had to move as quickly as possible to 'keep the lights' on for their customers and employees but are now facing the task of permanently re-engineering technology, process and workplace structure to navigate the permanent change COVID-19 has brought.

WILL THINGS GO BACK TO A 'NEW NORMAL' IN 2022?

When it comes to the cybersecurity landscape, the challenges that businesses will face in 2022 are profoundly different to those they faced pre-pandemic. For many there has been a fundamental cultural and philosophical shift in operations which will see organisations having to manage hybrid working arrangements where mobility will be key. This means the old cybersecurity 'fortress' mentality of securing systems will become obsolete and managing different access points on a permanent basis will be the new norm. New risk items such as geo-velocity risk need to be taken into consideration now.

WHAT IS THE MAJOR POTENTIAL TECH PAIN POINT THAT WILL FACE ALL ORGANISATIONS LARGE AND SMALL IN 2022?

Organisations will have to learn how to navigate the merging of Operational Technology (OT) and Information Technology (IT). Historically OT and IT have been managed separately, but the rollout of 5G and its increased speed and capability will see more and more connected devices, meaning OT and IT will rapidly become entwined. This will raise major budget and technology considerations (not to mention heightened security risk). For example, speaking recently to a CTO in the logistics business, he noted that in the last year alone hundreds of sensors were added to warehouses by the operational team without informing the IT team. This created hundreds more access points that could be leveraged for a cyber-attack.

Often IoT devices are being added for enhanced data collection capabilities, but the data needs to flow through all the way to corporate information systems to be analysed and used for various purposes. Front-end OT device breaches can therefore lead to compromised backend IT systems.

HOW CAN I.T. HAVE A GREATER IMPACT ON ORGANISATIONAL EFFICIENCY IN 2022, AND WHO (CEOs, CIOs) SHOULD LEAD THE CHARGE?

As technology now underpins almost every touchpoint of an organisation, IT has a real opportunity to impact organisational efficiency if working practices can align to speed, agility, creativity, and innovation. To have real impact though, it must become truly embedded in the business and in the boardroom. This requires a strong CEO mandate and a willingness from all to embrace organisational change. I'm working with some forward-thinking companies who have upended the way different aspects of IT are managed (separating innovation and cybersecurity from day-to-day IT operations for example) and it's going to be interesting to see where the optimal organisational structure lands.

Thomas Fikentscher is responsible for driving strong customer and partner engagement and expanding CyberArk's emerging cloud business in the region. When it comes to cybersecurity, Thomas sees a significant opportunity to bridge the gap between technology jargon and business language. A big part of this is helping company leaders understand the importance of identity security to operational risk management.

TERRY GOODMAN

FOUNDER AND MANAGING DIRECTOR, INTECH SOLUTIONS

LEADERS IN TECHNOLOGY 2022

HOW HAS AUSTRALIA COPED WITH COVID-INDUCED CHANGES TO OPERATIONS AND WORKPLACES? WILL THINGS GO BACK TO A 'NEW NORMAL' IN 2022?

Australia quickly and effectively embraced a 'work from home' policy. A clear side effect of this was how we define a 'team'.

In the past, a team was typically a group of people who worked together from the same location. Now, the 'location' aspect has diminished and teams are formed of people from anywhere. Not only have boundaries between staff in different locations diminished, but so have the boundaries between internal teams and vendors who now work much closer than in years gone by.

Online forms of communications have also changed the dynamics of team leadership. Introverts now have a greater voice than they did in the past, and the dynamics, and resulting output, of a team have generally benefited from more even contribution from team members.

We will return to offices as people tend towards human face-to-face interactions, but the expanded, more inclusive and cross-geographic composition of teams will remain.

WHICH NEW TECHNOLOGIES WILL REACH CRITICAL MASS AND BECOME DOMINANT IN 2022?

Graph databases are rapidly gaining momentum, emerging from an origin of 'connecting dots' in law enforcement and intelligence agencies, to a data storage technology that enables the exploration of connections and relationships in a wide variety of contexts.

Graph databases work by storing the relationships along with the data. Instead of calculating and joining the relationship as relational databases must do, graph databases simply read the relationship from storage. Compared with relational databases, graph databases are often faster for associative datasets and map more directly to the structure of object-oriented applications. They can scale more naturally to large datasets as they do not typically need joint operations, which can often be expensive. Graph databases work best when the data you're working with is highly connected and should be represented by how it links or refers to other data, typically by way of many-to-many relationships.

WHAT IS THE MAJOR POTENTIAL TECH PAIN POINT THAT WILL FACE ALL ORGANISATIONS LARGE AND SMALL IN 2022?

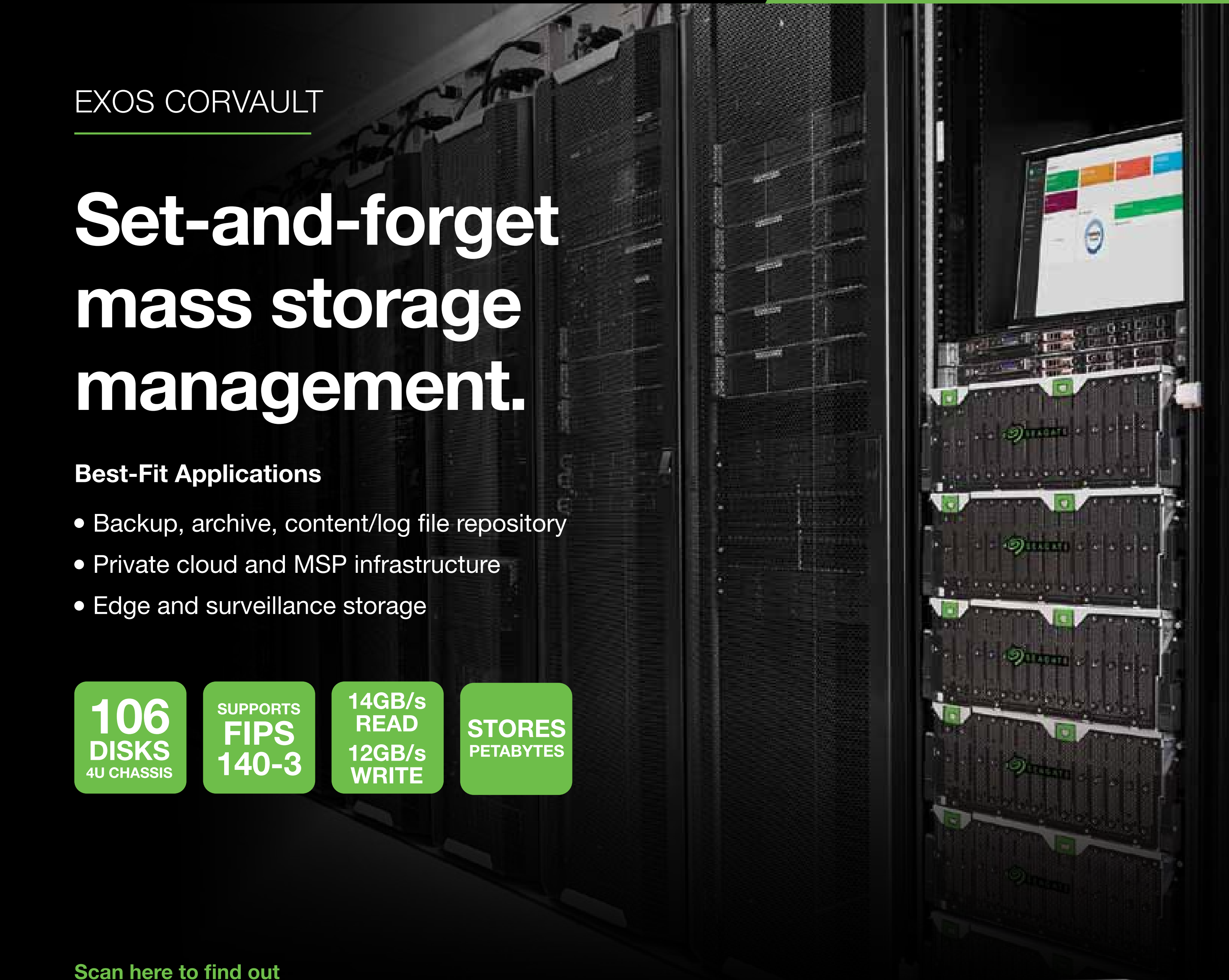
Security. A distributed and highly connected workforce has increased the attack surface area available to be exploited, and at the same time, threat actors are ever increasing their sophistication. The need to go above and beyond to implement secure practices is no longer the exclusive realm of the 'big end of town', now every business big and small needs to protect themselves from criminal cyber gangs.

WHAT'S ON YOUR TECH WISH LIST FROM GOVERNMENTS, INNOVATORS AND THE WIDER INDUSTRY IN 2022?

Integrated single sign-on security and password management. We all have so many passwords to manage — our work logins, bank account details, social media profiles and many more, each with two-phase authentication, varying minimum strength password policies and enforced password expiries. We must not write down our passwords, but so many people do. Password safes are commonly used amongst IT professionals, but scarcely used by anyone else.

Government and industry can solve this problem. The Australian Government is rolling out its myGovID system that provides better single source authentication for government systems, but this needs to be expanded for whole of economy use. It is my personal wish that government and industry will partner closely to enable Trusted Digital Identity (see: digitalidentity.gov.au/have-your-say) to become a reality across government and all industries.

Terry is the founder and managing director of Intech Solutions, an information management consultancy specialising in data quality. Since founding the company in 1996, he has guided development of the company and its products, and managed deployments at over 100 enterprise customer sites. Prior to his successful business venture with Intech Solutions, Terry was an information quality consultant with contracts held at Microsoft, Telstra Corporation, and the State Bank of NSW. Terry has a Bachelor of Science degree majoring in Computer Science and Mathematics.



SEAGATE

LEADERS IN TECHNOLOGY 2022

JEFF PARK

COUNTRY MANAGER ANZ, SEAGATE TECHNOLOGY

WHAT IS THE MAJOR POTENTIAL TECH PAIN POINT THAT WILL FACE ALL ORGANISATIONS LARGE AND SMALL IN 2022?

Mass data is one of the biggest pain points that all organisations will face in 2022 and beyond. Data that is more dynamic and fluid can be employed in multiple environments and offers organisations considerable business value. However, data is more often sprawled across an organisation in endpoints (like IoT devices), the edge and multi-cloud cores and can become stuck between these layers due to technical issues. There is also a significant gap between how much data is created and how much enterprises can afford to store. It's essential we address the total cost of ownership of data storage and fix these data flows to support public safety video imaging, critical healthcare data transport, smart manufacturing and more.

HOW CAN I.T. HAVE A GREATER IMPACT ON ORGANISATIONAL EFFICIENCY IN 2022 AND WHO SHOULD LEAD THE CHARGE?

CIOs have become more empowered in recent years as organisations shift their thinking about technology expenditure from viewing it as a cost centre towards considering it as an investment with a strong ROI. It's a good news story for IT, with an increasing number of deployments in Government showing success, addressing public concerns and challenges more efficiently. Top of that list would be the use of IT to assist with the vaccine rollout — drawing on multiple data sources to drive efficiencies and to connect health records across Medicare and MyGov and into Service NSW.

HOW CAN I.T. BECOME MORE ENVIRONMENTALLY FRIENDLY, SOCIALLY RESPONSIBLE AND PRIVACY-CONSCIOUS IN 2022?

It's incumbent on us all to play our part and to think laterally about how we can contribute. At Seagate for instance, as well as using renewable energy and seeking power savings in our manufacturing processes, we have launched several product recycling initiatives. We call these circularity projects and we're working collaboratively with Dell, Google, and other supply chain partners to recycle rare earth minerals from magnets. To date, over 2.5 metric tons of scrap magnets have been recycled. We recently also started the recycling of HDD aluminium from the Dell program into our motor base assembly and over 25 metric tons of aluminium has been recycled.

WHAT'S ON YOUR TECH WISH LIST FROM GOVERNMENTS, INNOVATORS, AND THE WIDER INDUSTRY IN 2022?

Top of my list would be improved support for both Australian startups and budding entrepreneurs. Too many are turning internationally for support and mentoring because there aren't enough foundations or facilities to nurture them. I'd like to see more companies open intern programs that welcome young talent into their workspace. Government should also play a greater role with subsidies, funding and programs, just as they do for apprenticeships.

Next would be improved broadband network infrastructure that addresses our geographical challenges. Today it seems like it will take a miracle to bring it up to speed, yet 20 years ago carrying a handheld device with all your personal medical and financial information, which also allowed you to video call around the world was the stuff of science fiction. Ironically the broadband infrastructure bottlenecks in Australia create more opportunity for companies like Seagate, because on-premises storage is still significant. This is quite the opposite to other regions around the world where cloud-based storage is our primary business.

Jeff joined Seagate in South Korea in 2004 to manage the channel. In 2007, he relocated to Australia, leading Seagate's Australian channel distribution business, before launching its surveillance and then consumer businesses, which took the company to market leader in ANZ. In 2019 he was appointed Seagate Country Manager ANZ.

CHRIS PECK

EXECUTIVE GENERAL MANAGER PUBLIC SERVICES, SAP AUSTRALIA

LEADERS IN TECHNOLOGY 2022

WILL THINGS GO BACK TO A 'NEW NORMAL' IN 2022?

We have seen a fundamental rethink of how to attract and retain talent over the past 18 months, as COVID-19 accelerated the public sector's understanding of its people and their skills. At SAP, we believe next year will be critical for our customers in terms of providing their employees with the right development and learning tools to provide career-building blocks inclusive of learning and development pathways. Linking these to job profile frameworks provides transparency across the workforce and, most importantly, career progression empowerment to every individual. This active support of employees through their professional growth will become the 'new' normal in 2022.

HOW HAS COVID-19 IMPACTED AUSTRALIAN SMBs AND HOW CAN THE PUBLIC SECTOR OFFER SUPPORT?

Running a small or medium-sized business (SMB) has never been more challenging. The COVID-19 pandemic continues to have a significant impact, with many business owners and managers accelerating digital strategies in response to the crisis. Companies are looking to external sources for help in their transition to digitisation, with about one in three taking advice from consultants and a similar number asking IT companies or governments for guidance. Public sector organisations need to remain open to questions from SMBs wondering where or how to start when it comes to digitising their business, particularly to ones already providing services to governments.

WHAT IS THE MAJOR POTENTIAL TECH PAIN POINT THAT WILL FACE ALL ORGANISATIONS LARGE AND SMALL IN 2022?

Cybersecurity and scaling it across the whole economy will continue to be the major pain point, and not just for large government agencies and corporates. Delivering this is only possible by moving solutions into the cloud and SaaS solutions which allow service providers to support cybersecurity for their customers. It is important to note that cybersecurity should not be solely seen as a technical problem to solve — there are no silver bullets. In addition to technical solutions it also requires training and education across an organisation on best-practice cybersecurity hygiene and management of the issue within risk committees.

WHICH NEW TECHNOLOGIES WILL REACH CRITICAL MASS AND BECOME DOMINANT IN 2022?

E-invoicing is not a new technology, but it has the potential to deliver large productivity benefits to the Australian economy in 2022, with the Australian Government investing $15.3 million to increase awareness and adoption. We commissioned a recent study on "The Connected SMB" which found that switching to e-invoicing could deliver Australian SMBs savings of up to $40,320. Payment times and security are also improved.

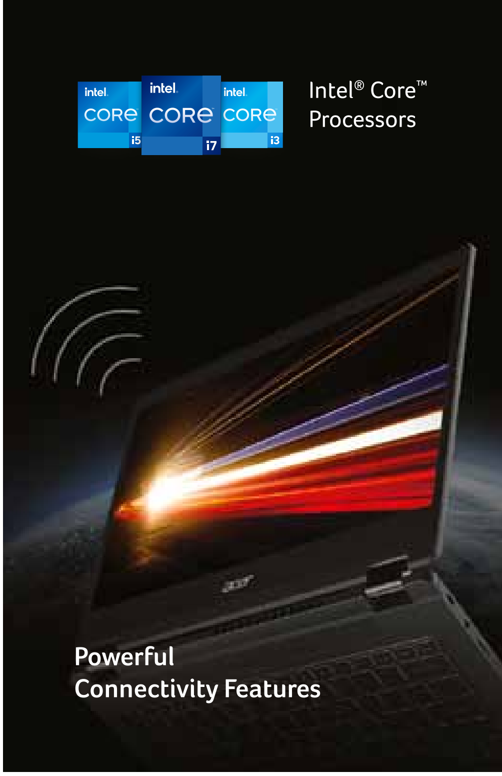
WHAT'S ON YOUR TECH WISH LIST FROM GOVERNMENTS, INNOVATORS AND THE WIDER INDUSTRY IN 2022?

Accelerate the adoption of digital technologies, like artificial intelligence, and the transition of government and business services to the cloud. Cloud offers lower cost of ownership, more convenient access, improved cybersecurity, scalable compute and automation. This allows organisations to become more proactive, foresighted and data-driven, with greater focus on citizens and customers.

Chris Peck is Executive General Manager, Public Services at SAP Australia. In this role, he works with the Australian Public Sector on digital innovation and transformation programs, as well as providing strategic advice, to ensure agencies take advantage of intelligent technologies to become more proactive, automated, foresighted, data-driven and citizen-focused.

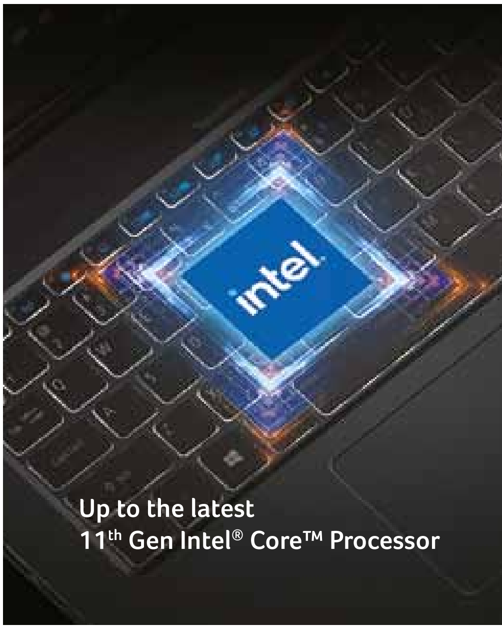
TravelMate Spin P4

PREMIUM NOTEBOOK FOR PROFESSIONALS



Intel® Core™ Processors

Powerful Connectivity Features



Up to the latest 11th Gen Intel® Core™ Processor

Built-to-last Military Grade Durability

ROD BASSI

OCEANIC SALES DIRECTOR, ACER

LEADERS
IN TECHNOLOGY
2022

HOW HAS AUSTRALIA COPED WITH COVID-INDUCED CHANGES TO OPERATIONS AND WORKPLACES? WILL THINGS GO BACK TO A 'NEW NORMAL' IN 2022?

We have never seen a time where so many people are required to work from their home offices or a hybrid work environment. All of which is made possible by the technology available to us today. There is a general discussion around whether there will be a 'new normal' where employees no longer commute to an office and collaborate with their colleagues virtually instead.

We will most likely see a more refined hybrid work environment where employees enjoy the flexibility of working from home, with offices adapting to meet a new set of requirements.

WHICH NEW TECHNOLOGIES WILL REACH CRITICAL MASS AND BECOME DOMINANT IN 2022?

Business leaders around the country are now taking a deep breath whilst preparing for the journey ahead. With a hybrid work environment becoming a new norm in 2022, we have seen an escalation of the adoption of digital technologies to facilitate a flexible and agile workplace.

In Australia, organisations are embracing the hybrid approach to remote work by providing the flexibility and the technology infrastructure to empower their employees digitally.

This means that business notebooks equipped with the right technologies to deliver high-performing portable devices will dominate in 2022. This will come in the form of powerful multi-core processors packed into thin ultralight laptops with all-day battery life to enhance employees' work-from-anywhere experience, driving the emergence of a new era of work.

WHAT IS THE MAJOR POTENTIAL TECH PAIN POINT THAT WILL FACE ALL ORGANISATIONS LARGE AND SMALL IN 2022?

The movement towards hybrid and remote working was as sudden as it was unprecedented. However, the shift towards virtual collaboration between teams and employees was not without its fair share of challenges that left staff in organisations with outdated technology.

This meant employees weren't equipped to handle the nature of hybrid work — resulting in situations where work devices would be out of battery after multiple video meetings or issues with poor home internet connection.

Acer has launched a new line of business laptops in the Acer TravelMate Series to support a productive hybrid work environment and address pain points. With features to enhance security, virtual collaboration and out-of-office productivity, the TravelMate business laptops offer a seamless working experience, whether in the office or from home. In addition, the lightweight and slim designs ensure that they are easy to carry and can be easily paired with an external monitor at a workstation.

HOW CAN I.T. BECOME MORE ENVIRONMENTALLY FRIENDLY, SOCIALLY RESPONSIBLE AND PRIVACY-CONSCIOUS IN 2022?

In 2022, we believe that there will be a continuing trend of environmentally friendly sustainable technology. Recently, we joined the RE100, a global initiative that brings together 300 of the world's most influential companies committed to 100% renewable electricity.

Our efforts towards a balance in finding integrated and innovative solutions while respecting the planet gives life to a unique platform of its kind. Earthion is a blend of the words "Earth + Mission" and combines the strengths of our company, our supply chain partners, consumers (channels) and our employees.

Our first step towards pioneering a fully green PC begins with the Acer Vero, a suite of eco-friendly products covering the Aspire, TravelMate and Veriton range. We have designed Acer Vero products to align with the core values of eco-minded consumers whilst meeting the significant list of environmental and socially responsible criteria from production to recycling.

With Acer's Earthion initiative and Acer Vero product range, we believe this will be a big step towards a cleaner and greener tomorrow for future generations.

Rod Bassi has been a senior executive with Acer for over 15 years, and as Oceanic Sales Director he oversees overall sales strategy across all market segments. He previously held the key strategic portfolio roles, General Manager of Commercial Sales, General Manager of Consumer Retail Sales and Country Manager of Acer New Zealand.

Connectivity: The essential framework for government transformation

Daniel Polomka, Regional Sales Manager ANZ, Cradlepoint

Every section of government has a responsibility to provide consistent services and keep citizens safe. Across Australia and New Zealand, government workers often deal with the unpredictability of whether a wired link is available or if it will be able to support the latest advancements in technology. In many instances, government departments are enabling the rapid rise of govtech with wireless broadband solutions.

Using LTE and 5G improves agility, flexibility, and resiliency in a variety of situations, including the following networking use cases.

Pop-Up Networks

For agencies and emergency services that are constantly on the move, it is critical to have a network that is secure and reliable but also easy to deploy quickly.

Pop-up LTE solutions enable on-demand, instantly deployed wireless connectivity for a variety of operations ranging from pandemic testing clinics to maintenance of an aircraft. By using cellular broadband, government workers complete the job anytime without relying on another organisation's network.

Remote Work from Anywhere

For government employees with high-bandwidth technology needs at home during the pandemic, providing cloud-managed LTE routers for remote work enables a dedicated network — isolated from the user's home network — that the IT team can centrally control without on-site intervention. The agency can monitor and control network connection performance and information security while staff members focus on completing their work.

Disaster Response Kits

With no time to waste during any type of emergency, there is an urgent need for Internet connectivity to ensure life-saving work can start immediately. Disaster response kits with built in LTE provide a flexible and on-the-go network within a ruggedised case that is easy to transport and can be used within the most austere environment.

Smart Bases

Military bases are becoming more advanced. Base commanders are looking to create operational efficiencies while also reducing costs without sacrificing mission readiness. Deploying Internet of Things (IoT) devices and applications requires network solutions that seamlessly connect numerous things

©stock.adobe.com/au/Peera

and that can be easily managed by IT staff working anywhere.

In examples like monitoring fuel distribution locations, connecting surveillance, security equipment and drones; using 4G LTE as the primary link instead of wired broadband allows for high availability and low latency for these constantly evolving technologies where a wired broadband connection may not exist. This helps avoid large amounts of downtime and costs.

Mobile Command Centres

For first responders, a fast response time is critical to saving lives, preventing a fire from raging out of control, or delivering emergency medical assistance. Any interruption in connectivity that delays critical information from getting where it is needed can put first responders, the public, and property at risk.

Technology that can help emergency services agencies secure and access data has grown in sophistication. There has been an expanding variety of emergency services applications of cellular connectivity in the field. Fire vehicle telemetry measures the volume of water a particular fire engine holds, and sensors on hoses that measure the volume of water passing through the hose over time, therefore enabling planning ahead and continuous effort where it's needed. Another example is the use of IP cameras for live video streaming from the front lines of natural disasters. Emergency services can assess how to ensure safety for personnel and what resources may be required at a particular site or incident. In the police environment, bodycams and holster sensors help protect officers as well as citizens.

Reliable connectivity is essential for emergency services agencies. Without a reliable and secure LTE and 5G network, emergency services won't be able to take advantage of the connected technologies available to make their jobs more effective and efficient.

Smart Cities

The definition of "Smart City" is broad, from roadways with sensors embedded in the ground and connected equipment for emergency services like police departments, to connectivity in schools and healthcare. While 'smart cities' covers a vast number of applications, the benefits of these technologies are easily seen to increase operational efficiency for governments — much of which is based on actionable IoT data — and improved services and quality of life for citizens.

Governments in other regions are already using 4G LTE and 5G to provide the reliability, visibility, and flexibility necessary to keep smart city edge technologies connected to agency networks at all times. Some examples of wireless connectivity in a smart city context:

- Schools — Whether on campus or on the bus, students are benefitting from LTE solutions that provide constant access to WiFi and to the swiftly expanding number of online education apps that are part of their day-to-day learning.
- Video Surveillance — With remote access to video surveillance, agencies can capture and analyse video footage to pinpoint and prevent theft, illegal dumping, and other suspicious activity. As 5G rolls out and evolves, live streaming of surveillance footage will become more common.
- Public Transit — Vehicle tracking, telematics, real-time route data for passengers, passenger WiFi, on-board IP surveillance, and digital ticketing are among the many connected technologies that can be used on today's city buses. Transit fleet managers can also use cloud management tools to make firmware, configuration, and security updates without having to bring every vehicle to headquarters.

Cradlepoint's NetCloud Service and wireless edge routers and adapters unlock the power of LTE and 5G to extend network access anywhere. Governments can depend on Cradlepoint's wireless edge solutions in any environment, from military bases and disaster response to offices and remote work, Cradlepoint provides agencies with highly secure and reliable access to mission-critical information and applications.

cradlepoint

Cradlepoint Australia Pty Ltd
www.cradlepoint.com/au

ANDREW BUD

FOUNDER AND CEO, IPROOV

LEADERS
IN TECHNOLOGY
2022

WHICH NEW TECHNOLOGIES WILL REACH CRITICAL MASS AND BECOME DOMINANT IN 2022?

Genuine presence assurance will become dominant in how organisations verify user identity online. The ability to tell that an online user is the right person, but also that they are real and authenticating in real time is game-changing for public sector agencies. The ATO introduced genuine presence assurance this year to securely verify citizens setting up their myGovID, and it's easy to see why: it has the convenience that other liveness solutions offer, with added security, inclusivity, privacy and scalability. Around the world, government departments are now able to move even the most secure processes online and give remote access to citizens who only need a device with a user-facing camera to complete an effortless face verification.

WHAT IS THE MAJOR POTENTIAL TECH PAIN POINT THAT WILL FACE ALL ORGANISATIONS LARGE AND SMALL IN 2022?

COVID has acted as an intensive lab for cybercriminals, just as it has accelerated the delivery and uptake of digital services. Fraudsters have been able to probe for weaknesses in verification methods and hone new skills on how to successfully attack businesses and consumers. Those two elements create a major tech pain point for all organisations, who need to do two things simultaneously: deliver security capable of protecting against sophisticated cyber attacks that evolve all the time and also make it extremely simple for any user to access online services.

HOW CAN I.T. HAVE A GREATER IMPACT ON ORGANISATIONAL EFFICIENCY IN 2022, AND WHO (CEOs, CIOs) SHOULD LEAD THE CHARGE?

Government I.T. teams will have a greater impact in 2022 in enabling citizens to interact effortlessly and whenever is convenient for them and in enabling employees to work from home securely with appropriate levels of security and access.

The past two years have seen a mass migration to home working. In 2022 there will be a huge need for more unified remote-work authentication solutions as the hybrid-working world matures. A reliance on BYOD puts core enterprise security at risk and we can expect to see more device-agnostic biometric authentication solutions deployed that can enable employees, contractors and suppliers to work more easily and securely across multiple devices. This frees workers and employers from the vulnerabilities and complexity of password management, while simplifying login to enterprise applications across environments.

WHAT'S ON YOUR TECH WISH LIST FROM GOVERNMENTS, INNOVATORS AND THE WIDER INDUSTRY IN 2022?

I'd like to see government agencies build on the progress made during the pandemic in providing citizens with more self-serve access to government services. I'd also like more organisations to understand that we're in an arms race with cybercrime. It's not going away on its own and it's not going to stay static while we work out what to do about it — cybercriminals are constantly evolving and changing their tactics. Governments must invest in technology to get ahead and stay ahead within their own infrastructures, but they must also hold wider industry to account. For example, if one bank falls prey to a money-laundering scam, it's not just the bank that suffers: the proceeds of organised crime cause untold harm in society. We must find ways to get beyond passwords and other insecure security methods, and biometric authentication will play an important part in that.

Andrew Bud CBE is founder and CEO of iProov, provider of face authentication and liveness services to the private and public sectors worldwide. iProov has pioneered the delivery of Genuine Presence Assurance, providing strong verification that an online user is real and authenticating in real time. Customers include the ATO and the NHS.

CIVICA

{ Our smart software is helping deliver the public services of the future.

Across the public sector and regulated markets, we support local and regional government, health and social care, social housing and education, combining our global reach with local understanding.

Our 30+ years of sector experience sets us apart.

With a customer focus and track record of delivery, we provide the smart software and cloud services which help public service providers around the world achieve better outcomes for people and communities.

civica.com

BRETT BARNINGHAM

MANAGING DIRECTOR LOCAL AND STATE GOVERNMENT, CIVICA

LEADERS IN TECHNOLOGY 2022

HOW HAS AUSTRALIA COPED WITH COVID-INDUCED CHANGES TO OPERATIONS AND WORKPLACES?

The response varied greatly due to differing levels of investment and preparedness that the organisations had taken. Some were able to pivot quickly and provide operational and citizen support very easily, while others were slower as they had to spend time getting the fundamentals into place to make the necessary changes. Overall, councils have been incredibly supportive of their communities and their staff, navigating what's been an incredibly difficult period.

WILL THINGS GO BACK TO A 'NEW NORMAL' IN 2022?

At this stage I'm not sure what the 'new normal' looks like, and I think it's going to vary depending on the communities that our local government are serving. One of the key takeaways from the last 18 months is that our organisations need to have higher levels of agility and adaptability, so we can adjust to whatever the new normal might be with greater ease and speed.

WHAT IS THE MAJOR POTENTIAL TECH PAIN POINT THAT WILL FACE ALL ORGANISATIONS LARGE AND SMALL IN 2022?

Technology is becoming more pervasive and accessible in our communities, both industrial and residential. Local governments need to solve how to interact and leverage the information from increasingly disparate technologies to gain insight on their communities to ultimately make better, data-driven decisions. The technical, security and privacy complexity will continue to grow and be a pain point for many organisations.

HOW CAN I.T. HAVE A GREATER IMPACT ON ORGANISATIONAL EFFICIENCY IN 2022, AND WHO (CEOs, CIOs) SHOULD LEAD THE CHARGE?

Technology can and is often used as part of a business improvement program, removing complexity and human cost. It can also provide greater access to citizens, and more broadly, community data which can be used for better planning and service delivery. To have the greatest impact requires change throughout an organisation including I.T. — but also includes people and processes, and therefore the vision and the ownership of this type of change should be led by the CEO.

HOW CAN I.T. BECOME MORE ENVIRONMENTALLY FRIENDLY, SOCIALLY RESPONSIBLE AND PRIVACY-CONSCIOUS IN 2022?

Transparency and user choice need to be central components of the I.T. solution giving stakeholders the ability to not only consent but also understand the broader use or implications of what they are engaging with.

WHAT'S ON YOUR TECH WISH LIST FROM GOVERNMENTS, INNOVATORS AND THE WIDER INDUSTRY IN 2022?

I'd love to see the wider use of edge technology being used in everyday life. It doesn't have to be a single big tech project — instead I want to see local governments leveraging the tech that the private sector is already using on a daily basis. For example, AI or visual recognition software to help us simplify processes and make fast decisions that deliver better outcomes for our communities.

Brett Barningham has over 15 years' experience in the technology industry providing enterprise software, cloud solutions and managed services helping organisations improve their businesses. He brings a passion for achieving through people, with a strong focus on innovation, organisational values and the customer. He believes that innovative and intelligent technology can transform the way we do things.

Tricentis

Speed changes everything.

We help enterprises accelerate their digital transformation with an AI-driven, end-to-end testing and automation platform.

With Tricentis, you don't just release software. You unleash it.

Tricentis | +61 2 8458 0766 | office@tricentis.com | tricentis.com

KARL WOOD

DIRECTOR OF FEDERAL ACCOUNTS APAC, TRICENTIS

LEADERS IN TECHNOLOGY 2022

WHAT'S ON YOUR TECH WISH LIST FROM GOVERNMENTS, INNOVATORS AND THE WIDER INDUSTRY IN 2022?

From the industry overall: fewer acronyms would be a good start. Next would be a shift towards the simplification of solutions, making tech easier for those with true business knowledge to implement and run successfully. For the government — the greatest challenge will be finding a way to simplify their processes so that tech can do more for them. The high customisation levels required to meet different department workflow and process demands results in solutions that are harder to support and ultimately more expensive. As tech providers, it is our responsibility to produce software, but also to listen and work collaboratively with departments to ensure the best solutions can be deployed with the least amount of customisation required. This will lead to solutions that are easier to support and faster to adapt to market changes.

HOW CAN I.T. HAVE A GREATER IMPACT ON ORGANISATIONAL EFFICIENCY IN 2022, AND WHO SHOULD LEAD THE CHARGE?

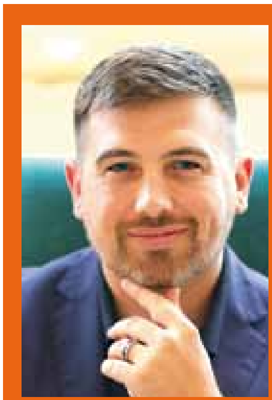
By removing the existing disconnect between those in lower and mid-level staff and the executive leadership team in departments, I'm confident that government can identify some game-changing efficiencies. Those staff that are on the ground most often have the best insights and ideas, but they rarely share them because they are afraid to rock the boat or are simply bogged down in work or customer processing. Implementing systems to capture feedback from frontline staff will potentially have a much better impact on organisational efficiencies than bringing in an external consultant to identify issues. It's a cultural issue that needs to be led from the top.

WHAT IS THE MAJOR POTENTIAL TECH PAIN POINT THAT WILL FACE ALL ORGANISATIONS LARGE AND SMALL IN 2022?

I anticipate that those who've invested in the well-hyped ML and AI solutions for complex deployments up front will be very disappointed. The reality is that both are incredibly useful for isolated use cases with a specific purpose, but not suited to completely solve enterprise-sized problems out of the box. We saw this with the initial deployments of RPA two years ago — isolated process usage delivered excellent results, but when you try and scale fast and wide there are serious disconnects. I think we'll see a fall back to manual processes and more resources and people required to manage the issues, especially given how reactive our response to COVID has been. Until the technology and processes align to allow interoperability and integration between departments, using ML and AI for overly complex online services and digitisation will be a problem that government will wrestle with.

WILL THINGS GO BACK TO A 'NEW NORMAL' IN 2022?

I suspect the new normal began long before COVID hit us. In early 2019 we had already seen a significant shift in operations and workflow, with a shift to integrate flexibility into government departments. This only amplified through 2020 and 2021 to the extent that we saw our Tricentis software testing software being used by government staff working remotely — a definite first. As we move into 2022, this will continue, and government will be scrambling to attract talent — alongside private enterprises — and seeking to balance the need to deliver secure and privacy-compliant remote workplaces to offer flexibility for workers.



Karl Wood is Tricentis's Director of Federal Accounts APAC, specialising in software development, solution architecture and quality assurance for government, finance and consulting. He has been a customer, supplier and consultant across multiple digital transformations, which has given great insight on common hurdles and developing industry-agnostic complex solutions.

JASON DUERDEN

REGIONAL DIRECTOR, SENTINELONE AUSTRALIA AND NEW ZEALAND

LEADERS IN TECHNOLOGY 2022

HOW HAS AUSTRALIA COPED WITH COVID-INDUCED CHANGES TO OPERATIONS AND WORKPLACES? WILL THINGS GO BACK TO A 'NEW NORMAL' IN 2022?

Australia, like all countries around the world, aggressively pivoted to remote working in 2020 due to COVID-19. Economic data suggests Australia has coped well with the adjustment with employment, and growth rates were relatively stable during the period. Industries such as hospitality and entertainment inevitably suffer as a result of lockdowns. Today, we are seeing a strong return to 'new normal' business operations and strong demand for flexible work at home arrangements alongside office work arrangements. Physical dependencies will no longer govern the workplace creation of 2022; people and talent enabled by online systems will be at the forefront of that requirement.

WHICH NEW TECHNOLOGIES WILL REACH CRITICAL MASS AND BECOME DOMINANT IN 2022?

Artificial intelligence for automation will reach critical mass and become more dominant in 2022. Over the last few years we have seen the rapid rise of automation to increase efficiencies in things like customer service, self-service and rapid response. This is becoming 'normalised' as an expectation with more and more organisations adopting AI for automation. Whilst perhaps not 'new', the rapid adoption of AI for automation is new and will break into new fields including cybersecurity.

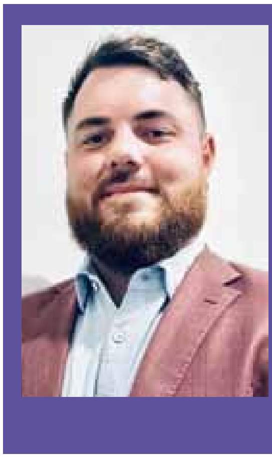
WHAT IS THE MAJOR POTENTIAL TECH PAIN POINT THAT WILL FACE ALL ORGANISATIONS LARGE AND SMALL IN 2022?

Software vulnerabilities. Now more than ever, supply chain risk via software vendors is at an all-time high. Criminalisation of IT has rapidly increased over the past 10 years, beyond just nation state on nation state espionage, to full-scale ransom, high-value targeting and data exfiltration. Outside of stolen passwords and social engineering, exploitation of vulnerabilities in software is a huge risk facing organisations in 2022. The recent examples of Microsoft and SolarWinds vulnerabilities being exploited show this is a targeted area.

WHAT'S ON YOUR TECH WISH LIST FROM GOVERNMENTS, INNOVATORS AND THE WIDER INDUSTRY IN 2022?

Automation and transparency.

There are many services and industries in our lives today that will benefit from automation, to reduce costs, reduce emissions, provide new opportunities for people in new industries — renewable energy being one and cybersecurity being another. I wish for Australia to be a global leader in these fields. Within transparency, human beings are inherently sceptical of technology because most of us don't understand it. Over the last 20 years, there have been numerous examples of big tech and governments walking the fine line of what's right and wrong with regards to data usage and collection. I wish big tech and governments to be ethically responsible and think... "just because we could, doesn't mean we should". Economics drives all decisions; 2022 will be a pivotal year in determining what the future of post COVID-19 society looks like and what's deemed important. Above all, securing our digital way of life is critical to the foundation of a stable and productive society.



Jason Duerden is the Regional Director for SentinelOne Australia and New Zealand, responsible for building and executing the business across Australia and New Zealand. Jason brings over 10 years of leadership, business management and technology acumen experience to SentinelOne with domain knowledge in the cyber arena and is an MBA candidate.

LLOYD EVANS

LASTPASS IDENTITY LEAD, LOGMEIN

LEADERS IN TECHNOLOGY 2022

HOW HAS AUSTRALIA COPED WITH COVID-INDUCED CHANGES TO OPERATIONS AND WORKPLACES? WILL THINGS GO BACK TO NORMAL IN 2022?

Over the past two years we've discovered a lot of new ways of working out of necessity. First, not being able to work face to face challenged the way we collaborate. Organisations were required to put substantial effort into integrating their virtual meeting solutions with technologies such as instant messaging and live document sharing to help people to work asynchronously, while balancing the 'working from home' lifestyles (homeschooling, remote locations, disparate time zones, etc). Second, the perimeter of the office has been redefined by employees working from their home offices. People are accessing their work applications using unsecured networks or their own devices, and this has driven organisations to implement tools to help adequately manage the identity of their employees while providing safe access to sensitive information. Last, with the increased use of work on personal devices in a remote setting, organisations have implemented technologies to ensure their employees are supported at all times and from anywhere. This is especially important for government organisations as they ensure continuity to the services they provide for their constituents while keeping everyone safe.

WHAT IS THE MAJOR POTENTIAL TECH PAIN POINT THAT WILL FACE ORGANISATIONS LARGE AND SMALL IN 2022?

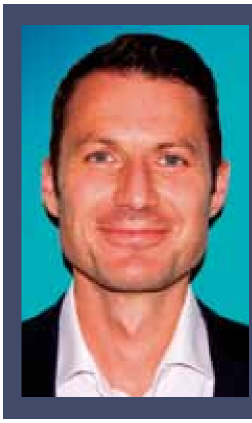
Based on the findings of the most recent Data Breach Investigations Report (DBIR) report produced by Verizon, 85% of the data breaches globally occur due to human error — most related to compromised or stolen credentials. This trend is consistent in Australia — the OAIC reported 62% of cyber incidents in 2021 were attributed to compromised or stolen credentials. It's a fact, hackers aren't hacking in, they are logging in, and password management is the Achilles heel of the cybersecurity landscape. Organisations across the region have recognised this risk and put in place several programs to help their employees to be educated about the multiple ways their personal data is vulnerable and can be used maliciously to breach corporate sensitive information. Institutions need to invest in solutions that help protect the digital identity of their employees. This can be achieved by integrating their existing single sign-on and multifactor authentication technologies with a password manager such as LastPass by LogMeIn.

HOW CAN I.T. HAVE GREATER IMPACT ON ORGANISATIONAL EFFICIENCY IN 2022, AND WHO (CEOs, CIOs) SHOULD BE IN CHARGE?

Organisational efficiently is a cross-functional effort. Leadership defines culture, and culture defines performance. All the leaders within the organisations need to work together to determine the vision and policies in which the employees will operate going forward (remote working, hybrid or full-time in the office). From that point of view, Leaders in I.T. need to take the necessary steps to build or rebuild the ecosystem with hardware and software to enable people to do their best work.

WHAT'S ON YOUR TECH WISH-LIST FROM GOVERNMENTS, INNOVATORS AND THE WIDER INDUSTRY IN 2022?

This year we've seen organisations embracing digital transformation like never before, this is also the case for malicious actors attempting to hack individuals' personal data. There is an opportunity for governments and leaders in IT to further implement programs to help their constituents be educated about how their personal data is vulnerable and the ways to fortify their digital footprint.



Lloyd Evans leads LastPass business for JAPAC. When he's not training for his next ultra-marathon, Lloyd enables organisations to elevate their security posture while saving money and time. A cybersecurity, cloud and technology industry veteran, Lloyd has previously held senior sales roles with Solar Winds, CBA, St. George Bank and Macquarie Bank.

TONY BAUMAN

COUNTRY MANAGER ANZ, VECTRA

LEADERS IN TECHNOLOGY 2022

HOW HAS AUSTRALIA COPED WITH COVID-INDUCED CHANGES TO OPERATIONS AND WORKPLACES? WILL THINGS GO BACK TO A 'NEW NORMAL' IN 2022?

In 2020 and 2021, employers have been faced with the challenge of providing a seamless and secure work experience to employees, irrespective of location and role. They were also tasked with embracing new technologies to support employees' productivity and general health.

Overall, A/NZ organisations have done well to pivot and support their people, despite changes to previous operational and workplace norms. This level of support will be the 'new' normal and will continue to stretch IT and HR teams. The workforce in 2022 will be driven by the need to balance the requirements of employees and the business, so it will include a mix of cultural and operational aspects.

WHICH NEW TECHNOLOGIES WILL REACH CRITICAL MASS AND BECOME DOMINANT IN 2022?

Cloud and security adoption will continue to accelerate to meet the 'new' normal business landscape, and create hybrid workplaces that cater to customers, supply chains and employees. Organisations must adapt to the concept of 'the anywhere customer' and 'the anywhere worker', enabling customers and teams to have the same experience regardless of where they are.

Security technologies to protect this 'new' normal business landscape from cyber attack will be broadly adopted to ensure appropriate protections are in place, and threats are identified and remediated prior to them causing disruption and harm.

WHAT IS THE MAJOR POTENTIAL TECH PAIN POINT THAT WILL FACE ALL ORGANISATIONS LARGE AND SMALL IN 2022?

The main pain point facing organisations is securing assets, data, customers, supply chains and employees — across cloud, data centre, IT/IOT and workplaces. On a weekly basis, we see threat actors across the globe turning up the tempo of their activity, and the impact of their attacks on corporations, governments and civilians. This isn't slowing down. Organisations need to make interactions frictionless across their business, while also establishing the security measures required to protect data and operations across their estate.

Another potential pain point is meeting obligations to regulatory requirements due to these cyber threats. There are many changes and new legislations coming from a government and regulatory level, such as the Security Legislation Amendment (Critical Infrastructure) Bill 2021. These changes could impact the cybersecurity investments required and reporting obligations of organisations, whether big or small.

HOW CAN I.T. HAVE A GREATER IMPACT ON ORGANISATIONAL EFFICIENCY IN 2022, AND WHO (CEOs, CIOs) SHOULD LEAD THE CHARGE?

What is most impactful is when you can map I.T. outcomes against business objectives and are able to identify risks and risk management requirements.

In terms of leading the charge, we need stronger board-level conversations to address new cyber threats and government and regulatory obligations. As the definition of critical infrastructure broadens, boards must understand and support CEOs and CIOs in their ability to protect their business.

WHAT'S ON YOUR TECH WISH LIST FROM GOVERNMENTS, INNOVATORS AND THE WIDER INDUSTRY IN 2022?

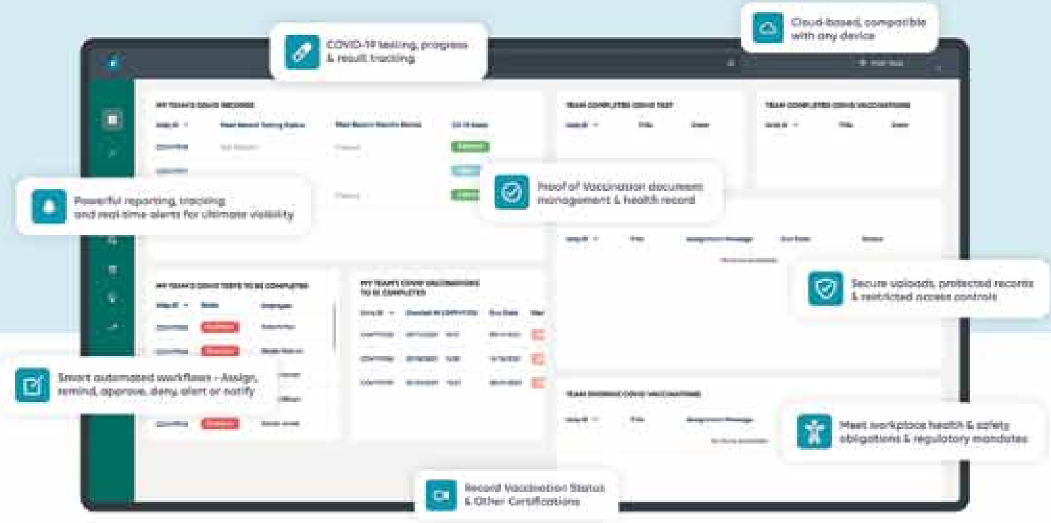
I'd like to see governments continue to support innovation in our country, and I'd like to see the wider industry increasingly focus on the real and persistent threat of cyber attacks that are impacting business, supply chains and our society. We need to continue to be vigilant.

Tony Bauman is Country Manager, Australia and New Zealand (ANZ) for Vectra AI. He is responsible for leading the field sales organisation across the region to expand Vectra's customer base in key vertical markets including finance, government and critical national infrastructure as well as driving sales via Vectra's partner ecosystem.

Introducing VaxSAFE

Workplace Vaccine & Test Status Tracking

Compliance Made Easy!



COVID-19 testing, progress & result tracking

Cloud-based, compatible with any device

Powerful reporting, tracking and real-time alerts for ultimate visibility

Proof of Vaccination document management & health record

Secure uploads, protected records & restricted access controls

Smart automated workflows - Assign, remind, approve, deny, alert or notify

Meet workplace health & safety obligations & regulatory mandates

Record Vaccination Status & Other Certifications

Effortless Compliance, Adaptive Safety

On the go test submissions

Live vaccination status

Is your business VaxSAFE?

VaxSAFE by Donesafe simplifies COVID-19 workplace tracking of vaccination and testing status all under one centralised cloud-based platform making return to work effortlessly compliant.

Trusted by Australia's Safest Workplaces.

COVIDSAFE + COVIDSAFE +

Request a live demo & find out more
vaxsafe.donesafe.com or call us on 1300 137 408

hsi donesafe
An HSI Company

MATT BROWNE

CO-FOUNDER & FORMER CEO, DONESAFE

LEADERS IN TECHNOLOGY 2022

HOW HAS AUSTRALIA COPED WITH COVID-INDUCED CHANGES TO OPERATIONS AND WORKPLACES? WILL THINGS GO BACK TO A 'NEW NORMAL' IN 2022?

Workplaces over the last decade have rapidly evolved, driven largely by the adoption of cloud-based platforms and digital transformation initiatives. This has ultimately led to more flexible forms of working from 'hot desking' to remote working arrangements.

What we are seeing is that COVID-induced changes have simply accelerated this transition to a more permanent workplace change that have now become the 'new normal' as we head into 2022. How businesses evolve their workplace health and safety protocols to align with this 'new workplace' environment will be one of the key priorities for business and safety leaders in 2022. Given more stringent safe work obligations and mandates from regulatory bodies throughout 2021 for compliance, I expect OH&S to be a major operational focus in the coming year.

WHAT IS THE MAJOR POTENTIAL TECH PAIN POINT THAT WILL FACE ALL ORGANISATIONS LARGE AND SMALL IN 2022?

There is no doubt the concept of 'cloud first' is now a reality when it comes to tech strategy. The first pain point businesses will likely face will be around migrating off outdated on-premise infrastructure that currently supports core business systems as security, flexibility and accessibility become increasingly a priority.

The second pain point will be around creating a 'connected' workplace ecosystem where digital workflows are seamlessly connected across various systems alongside hardened end-to-end security and privacy measures. Essentially creating a true paperless organisation is now a reality as security and productivity 'anywhere' is the norm.

HOW CAN I.T. HAVE A GREATER IMPACT ON ORGANISATIONAL EFFICIENCY IN 2022, AND WHO (CEOs, CIOs) SHOULD LEAD THE CHARGE?

I.T. now plays a leading role as integrators within organisations as they become more digitally connected from the ground up. CIOs and CTOs are increasingly asked to play an 'enabler' role working with other functional leaders to ensure various platforms are seamlessly connected throughout the workplace.

That being said, functional leaders now need to collaboratively work across the business given the interdependence of various platforms, big data and security factors that play a critical part in all businesses regardless of industry or size.

HOW CAN I.T. BECOME MORE ENVIRONMENTALLY FRIENDLY, SOCIALLY RESPONSIBLE AND PRIVACY-CONSCIOUS IN 2022?

I.T. leaders must go beyond simply reducing the I.T. footprint of an organisation to looking at some of the broader strategic factors at play.

Data security alongside protecting both customer and employee privacy are critically important as all businesses naturally become data-led. This needs to be a prerequisite when I.T. leaders perform due diligence on new and existing platform choices.

Adopting an enterprise grade Environmental Health & Safety (EHS) software such as Donesafe is another way to centralise, manage and automate an organisation's objectives around achieving sustainability, risk and safety objectives.

Matt Browne is the co-founder and former CEO of Donesafe, a market-leading global EHS SaaS platform with 1.5million+ paying users. Matt took the business from launch in 2013 to the acquisition by HSI in 2020. He is on a mission to build greater technology efficiency and literacy.

3 Ways Government Employees Can Bolster Their Cyberhygiene

Leon Adato, Head Geek at SolarWinds

© Stock.Adobe.com/au/sutadimages

Security is everyone's responsibly — not just the IT team. This sentiment is especially timely in today's landscape, where cyberattacks are becoming more frequent, all-encompassing, and sophisticated.

Case in point, the latest SolarWinds Public Sector Cybersecurity Survey found untrained or careless insiders accounted for the most significant source (52%) of security threats. Sadly, this trend has continued for more than five years. This underscores the importance of shared responsibility when it comes to security and that the biggest threat could come from within.

A robust security strategy for government bodies should include changes at the organisational and individual levels. And to be clear, this is not to unduly scrutinise employees, but — given their level of access and privilege — to protect them and the organisation from attackers.

Here are three ways government employees can brush up on their cybersecurity skills, protecting the wider organisation in the process.

1. Take stock and assess

We all fall victim to this one — how often do we forget we have access to systems or applications we no longer use? Whether you've finished working on a project, changed your role, or moved departments, you could still have access to sensitive information that could be used if your access is compromised. Luckily, this should be an easy fix.

Take stock of everything you have access to and make a list of things you no longer need to do your job right now (remember, you can always get access again later if need be). Then work with your IT team to restrict your access to only what you need. Understanding and proactively managing your digital footprint is one of the easiest ways to limit risk exposure from attack.

2. Get privileges right

As mentioned above, users pose one of the biggest threats to government bodies, so agencies are increasingly adopting tools to verify user identity. This helps IT teams manage what systems each user should — and shouldn'tÂ — have access to.

The SolarWinds survey found identity and access management tools are heavily adopted (97%) and rated as the second-most-effective tool for application and network security behind endpoint protection software.

The same survey found over half of federal, state, and local government bodies use network segmentation and a zero-trust approach to manage user access. But achieving effective segmentation utilising this approach is more elusive than ever due to the growing number of systems, devices, and users. Implementing and maintaining zero-trust is also fraught with issues, mainly escalating costs and a lack of expertise.

Users can play their part by working with their manager to ensure they have access to only the necessary privileges to get their work done. If users need additional access, it can be granted on a temporary basis and should expire after a certain time (or when the task is complete, whichever comes first).

3. Separate work and home

Most of us have taken work home this past year, adopting a fully remote or hybrid setup as COVID-19 impacted business as usual. Although work may be done at home, keeping work and home data separate is critical.

Think of home like a remote site when assessing security parameters. For example, employees should ensure their router's firmware is up to date and they're using the WPA3 Wi-Fi protocol (which is more secure than the previous WPA2 standard). Then check firewall settings and turn off any open ports. Be sure to choose a complex network password that's long, unique, and uses a combination of letters, numbers, and special characters. If your organisation uses a VPN, employees should connect this way when at home. Lastly, avoid — at all costs Â— transferring work files to home devices or using email for sharing sensitive information.

Time for users to step up

Cyberattacks are on the rise and becoming more targeted. Individual users can play their part in the collective effort to beef up security by taking stock of their permissions, managing privileges, and keeping work and home separate (at least in a digital sense).

These small steps and behaviour changes can go a long way to improving the government's security preparedness.

SolarWinds
www.solarwinds.com

everbridge®

Keeping People Safe And Organisations Running. Faster.

What Everbridge Does

During public safety threats such as bushfires, earthquakes, terrorist attacks, a global pandemic, or severe weather conditions, as well as critical business events including IT outages, cyber-attacks, supply chain interruptions, all levels of government rely on Everbridge's SaaS-based Critical Event Management platform.

Everbridge's Critical Event Management Solutions:

+ **Business Operations**: keeping departments and operations running, faster
+ **Digital Operations**: protecting brand and reputation while providing resilience for IT systems
+ **People Resilience**: fulfilling duty of care for residents, remote and onsite employees, travelers, and field workers
+ **Public Safety**: Everbridge. Everywhere. Every time. Public Safety for every Australian
+ **Supply Chain Risk**: managing and optimising for risk to supply chains
+ **Smart Security**: smart automation, secure IoT management, big data, and advanced analytics

LEARN MORE AT
Everbridge.com

STEVE FOSTER

VICE PRESIDENT ANZ, EVERBRIDGE

LEADERS IN TECHNOLOGY 2022

HOW HAS AUSTRALIA COPED WITH COVID-INDUCED CHANGES TO OPERATIONS AND WORKPLACES? WILL THINGS GO BACK TO A ‘NEW NORMAL’ IN 2022?

When the pandemic first hit we all scrambled to adapt as teams were forced to work from home. Every store that sold tech was suddenly sold out of monitors, laptops, webcams, microphones and all the building blocks we needed to be predictive from home.

But as the pandemic continued, organisations adapted. Everyone started refining what was needed to make remote working not just possible but also convenient and productive.

The new normal of 2022 and beyond is the realisation that hybrid workplaces need not be feared. We’ve proven people are more productive and they offer significant organisational benefits in terms of employee wellness and reduced need for renting huge office spaces, saving the bottom line. There’s a new dynamic developing where people are being trusted to work remotely and that it’s possible to have great communication without needing to drive to an office or fly across a country of the world.

WHAT’S ON YOUR TECH WISH LIST FROM GOVERNMENTS, INNOVATORS AND THE WIDER INDUSTRY IN 2022?

A CEM platform that works with the Fusion Centre should be at the top of every organisation’s wish list. This is a risk-based, technology-delivered approach to identifying critical assets, the risks that can impact them and having automated processes that support people to ensure that the impact of a critical event is mitigated.

This requires a centralised tool that unifies all the requirements for an organisational-wide efficient response. Incident response in government agencies or private companies is often hampered by internal silos. Improved collaboration improves response times and fosters a shared vision of keeping people and places safer.

WHICH NEW TECHNOLOGIES WILL REACH CRITICAL MASS AND BECOME DOMINANT IN 2022?

Technology is developing rapidly. The building blocks are there for organisations to do almost anything they can imagine. But ensuring everything is running well and securely will become increasingly important.

At Everbridge, we provide a cloud-based Critical Event Management (CEM) platform that enables customers to see and anticipate various forms of disruption. We help businesses identify the assets that are most valuable to them and where the risks are. We define a critical event as something at the intersection of those two things.

We bring digital transformation to safety, security, and operational resiliency. Our aim is to mitigate and potentially eliminate the impact of a critical event on an organisation.

That means tracking globally, natural disasters, IT disruptions, civil unrest and other events that can impact operational safety and effectiveness so organisations can pre-emptively act to minimise impact.

HOW CAN I.T. HAVE A GREATER IMPACT ON ORGANISATIONAL EFFICIENCY IN 2022, AND WHO (CEOs, CIOs) SHOULD LEAD THE CHARGE?

The traditional approach to critical event management was very reactive. Something broke so we’d send experts in to fix it by following a procedure or playbook. But that doesn’t scale in today’s world. There are cybersecurity attacks every second. In Australia, critical infrastructure is attacked every 32 minutes. The reactive break/fix world does not exist anymore.

Customer expectations have changed with self-service citizen services. Technology needs to adapt but remain seamless to the user. That means you need a robust and scalable incident management solution that is futureproof and adapts with you.

The solutions obviously have a technology edge but initiatives must be business led and I.T. delivered. The CEO needs to lead this shift, run the initiative through the Chief Risk Officer and have it delivered by I.T. This is the Fusion Centre approach to CEM.

Steve Foster is VP ANZ at Everbridge. With a background in strategic business development and sales, Steve has over 15 years’ experience with multinationals in global and regional leadership roles, specifically in Cloud (Application Development/DevOps/SRE/ Automation) for SaaS, PaaS, and IaaS Solutions.

Looking for a better way to manage mobile devices? Look no further!

Automate Your Workflow

The FUYL Tower can work alongside your IT team and staff, helping maximise workflow efficiency. With seamless integration into your existing system, the FUYL Tower together with PC Locs Cloud can automate workflows by:

1. Allowing organisations to keep devices charged, secure, and tracked
2. Helping distribute devices from a central, safe, and accessible location
3. Creating accountability while ensuring your staff never slows

Eliminating manual workflow processes and simplifying the replacement of damaged, lost or forgotten devices saves time, money, and lessens the load on an already busy tech team.

PC Locs is an Australian owned company dedicated to the design, manufacture and functionality of the highest quality security, charging and management solutions for mobile device deployments. With over 23 years of experience in the industry and protecting millions of devices in PC Locs solutions throughout 20+ countries, we make our customers' lives easier by developing solutions with scalable and modular designs.

pclocs

Specifications and images are for illustration purposes only. Final products may differ. May not fit all devices. Please check the dimensions of the device and the product. Contact us for more details and compatibility.

JAMES SYMONS

CEO, PC LOCS

LEADERS
IN TECHNOLOGY
2022

WHICH NEW TECHNOLOGIES WILL REACH CRITICAL MASS AND BECOME DOMINANT IN 2022?

The COVID pandemic has accelerated the move to ‘contactless delivery’. The awareness of the need to social distance has led to a range of services that offer delivery without physical contact. At the basic end of the scale are home delivery services where packages/food are left at the door without the need for face-to-face contact. A growing sector is self-service delivery SMART LOCKERS operated by sophisticated cloud platforms that enable customers to access their delivery by PIN or other unique codes, such as the PC Locs Cloud managed FUYL Tower. Similarly, these smart lockers can also provide a contactless check in/check out system for organisations that wish to reduce cost and physical contact in device service scenarios.

WHAT IS THE MAJOR POTENTIAL TECH PAIN POINT THAT WILL FACE ALL ORGANISATIONS LARGE AND SMALL IN 2022?

With remote work becoming more commonplace since the beginning of COVID, the need for all employees to have access to stable and secure hardware and enterprise software is paramount. Downtime due to device service issues or software issues is always a problem, but more so with remote employees who cannot access support as easily as if they were onsite. Comprehensive helpdesk support is a necessity, backed by the ability to quickly access replacement devices, particularly for mission-critical devices. Strategically placed smart lockers that enable team members to quickly swap out faulty devices without the need for physical contact can significantly reduce risk and cost to organisations facing these issues.

HOW CAN I.T. HAVE A GREATER IMPACT ON ORGANISATIONAL EFFICIENCY IN 2022, AND WHO (CEOS, CIOS) SHOULD LEAD THE CHARGE?

The negative impact on organisational security from a less than clear focus on comprehensive cybersecurity policies/procedures moving into 2022 cannot be understated. From the CEO down, executive teams need to drive cybersecurity awareness through their organisations to the entire company to mitigate the risk of catastrophic business interruption. Comprehensive policies that protect the company and cover all areas of an enterprise from information security and internet usage to the physical security of mobile devices are crucial to ensuring business continuity. Information security breaches caused by the loss of theft of mobile devices is one of the main sources of data theft and must be protected against by ensuring that all devices are kept secure at all times.

WHAT’S ON YOUR TECH WISH LIST FROM GOVERNMENTS, INNOVATORS AND THE WIDER INDUSTRY IN 2022?

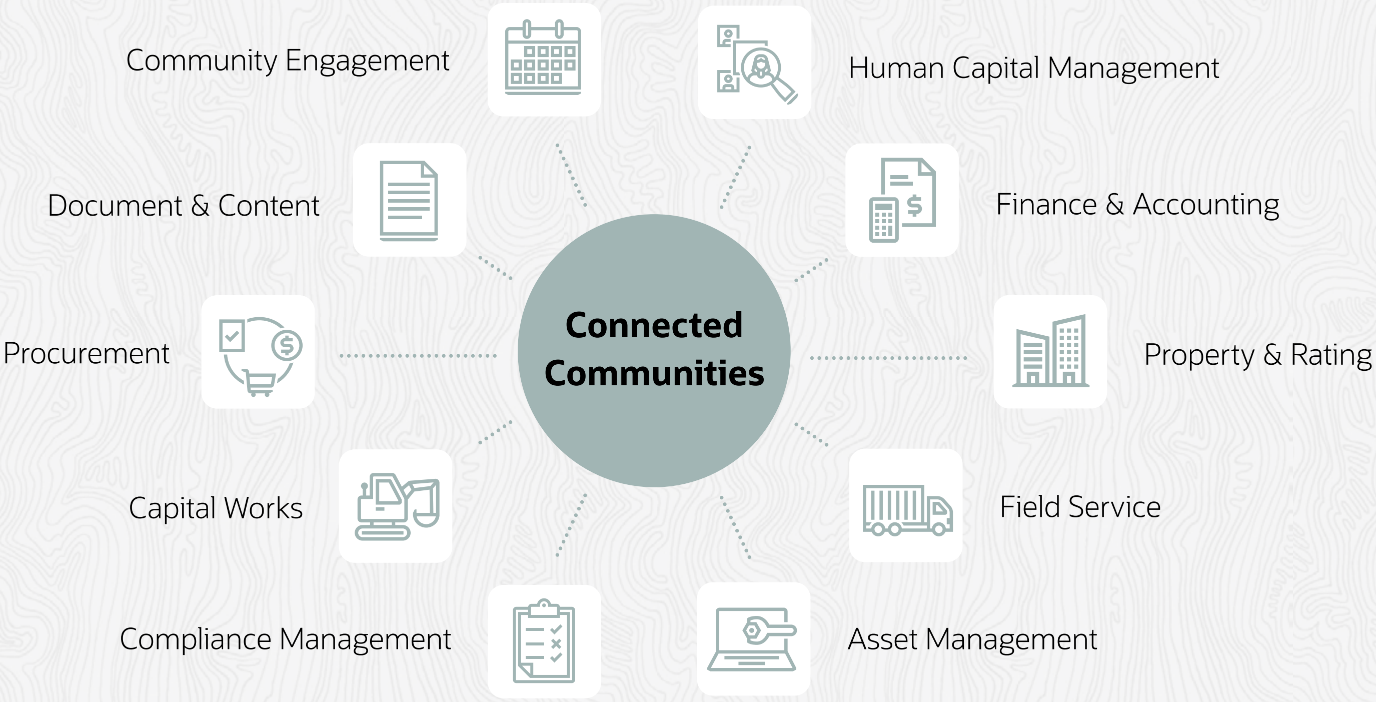
Boosting government initiatives that build a national infrastructure to support the Internet of Things and cloud/managed services across all sectors of industry and domestic use is vital. This would include ongoing development of a national 5G network and federal/state assistance to underpin efforts to counter the growing cybersecurity threat.

In 1998, James joined his father in building the family business, PC Locs. After becoming CEO in 2006, expansion became a focus for James, and now the company has offices worldwide, selling products and software services globally. Today, James is just as passionate and committed to providing the best possible hardware and software solutions for managing mobile devices.

Intelligent Councils, Connected Communities

Transforming Councils into Smart Cities and Communities.

Oracle provides local government with a complete integrated solution, servicing:



Connected Communities

Community Engagement

Human Capital Management

Document & Content

Finance & Accounting

Procurement

Property & Rating

Capital Works

Field Service

Compliance Management

Asset Management

CONNECT WITH US

blogs.oracle.com/oracle
facebook.com/oracle
twitter.com/oracle

SHANE BARTHOLOMEW

DIGITAL TRANSFORMATION LEADER, HUME CITY COUNCIL

LEADERS IN TECHNOLOGY 2022

HOW HAS HUME CITY COUNCIL COPED WITH COVID-INDUCED CHANGES TO OPERATIONS AND WORKPLACES? WILL THINGS GO BACK TO A 'NEW NORMAL' IN 2022?

Like other organisations, we needed to rapidly respond and make the changes that were needed to keep everyone safe. For us at Hume City Council this meant mobilising a workforce overnight to support working from home and enabling a VPN that was previously supporting 50 concurrent users to cope with an increase to 500. While taking care of the health and wellbeing of our staff, we also focused on our community. They looked to us for support and we were there for them — by helping individuals and families who were doing it tough, setting up vaccination hubs and working closely with community leaders to educate. In 2022 we are looking forward to welcoming staff back into our offices and embracing a new normal with a hybrid working arrangement.

WHICH NEW TECHNOLOGIES WILL REACH CRITICAL MASS AND BECOME DOMINANT IN 2022?

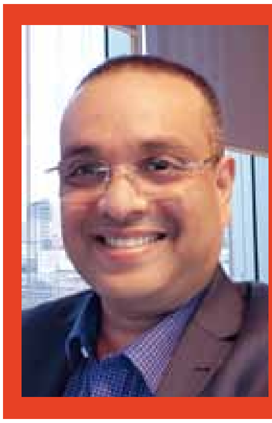
COVID notwithstanding, there has been a growing trend for organisations to embrace digitisation. The pandemic accelerated that change and it's gathering momentum. I think we'll see a continued growth in infrastructure as a service (IaaS) as well as software as a service (SaaS) — and a growing awareness of the positive trade-offs when moving to these technologies, whether it's scalability, reduced overheads, lower maintenance costs and/or greater security. For us, the value proposition includes security of our community's data, along with a higher level of service reliability. In 2022 we're delivering both. We are deploying a SaaS CRM system and will migrate most of our on-premises infrastructure to the cloud. Our staff will be able to service the community digitally, over the phone, across the counter or in the field through increased system capability and access to accurate data.

WHAT IS THE MAJOR POTENTIAL TECH PAIN POINT THAT WILL FACE ALL ORGANISATIONS LARGE AND SMALL IN 2022?

The pandemic has shown the tactical advantage of being digital ready. As more organisations embark on their digital transformation journeys as a matter of survival or smart business, an unintended consequence is likely be a global shortfall in I.T. talent to meet demand. The positive is that in I.T. our workforce is genuinely global. For Local Government I feel 2022 presents a slightly more nuanced set of opportunities. A big focus for our Council will be how we help our community recover after a very tough period and where we invest our resources will be influenced by this goal. We will not be alone, as other Councils also lean in to help in community recovery efforts. Being very clear about purpose and the tangible outcomes that need to be delivered is a helpful anchor and calibration point to have along the journey.

HOW CAN I.T. HAVE A GREATER IMPACT ON ORGANISATIONAL EFFICIENCY IN 2022, AND WHO (CEOs, CIOs) SHOULD LEAD THE CHARGE?

For I.T. the starting point is to understand who our customers are and what our purpose is in relation to the services we offer. Even when looking to deliver efficiencies, it is important to keep sight of who we are ultimately here to serve. For us here at Hume it is our community and in the first quarter of 2022 we are deploying a new Oracle-based CRM platform that will change how we serve them. Our new CX capability is underpinned by an omni-channel platform with access to a single-view repository containing all customer data within Council. Providing our customers with a more convenient and seamless way to engage with us 24/7, whilst also improving our internal operational efficiency with real-time access to a central, accurate repository of customer information. For us here at Hume City Council our digital transformation is leader led, starting with our CEO Sheena Frost, and is supported by our entire Executive Leadership Team.



Shane is an experienced leader with 20+ years' expertise in leading strategic transformational change across manufacturing and telecommunications sectors. Specialising in process improvement, data analytics and customer experience, he is known for driving strategic vision and transformational advances that generate solutions for complex issues with a focus on continuous improvement.

PUBLIC SECTOR IT SPEND TO GROW 8.8% IN 2022

© Stock.Adobe.com/au/immimagery

The Australian government sector will spend more than $15.5 billion in 2022, according to new forecasting from Gartner — an 8.8% increase on 2021 levels. The new figures include all levels of government — federal, state and local — but do not include the education sector.

According to the forecast, the software segment — including application, infrastructure and vertical-specific software — will experience the strongest growth in 2022 at 19.2%.

While devices experienced the strongest growth in 2021 as government organisations embraced remote work and connected public services, it will suffer the strongest decline of -5% in 2022. Telecoms services are forecast to decline for the second year in a row.

"Government technology spend in Australia is expected to continue upward for the next few years driven by key programs to progress the digital economy, strengthen national cyber response, adopt emerging technologies and address gaps in regulation to cover technology," said Brian Ferreira, Vice President, Executive Programs at Gartner.

"Consultation papers on AI, ethics, technology and human rights, blockchain and other emerging technologies are now firmly on the government's radar."

In 2022, increased investments in digital technologies will see governments in Australia spend 72% of total IT spending on IT services and software to improve responsiveness and resilience of public services (see Table 1). These include investments in enhancing customer and employee experience, strengthening analytical capabilities and scaling operational agility.

IT infrastructure and applications modernisation as well as digital government transformation will remain high government priorities in 2022. In Australia, the $1.2 billion Digital Economy Strategy announced in this year's federal Budget aims to support investments in emerging technologies and digital skills to advance Australia's position as a modern digital economy by 2030.

"As the Delta variant continues to create hurdles, government spending will increase on solutions to open up the Australian economy while we continue to live with COVID-19, particularly to drive vaccination validation, open up borders and unblock trade," said Ferreira.

Segment	2021 spend	2021 growth (%)	2022 spend	2022 growth (%)
IT services	6,001	7.0	6,435	7.2
Software	3,935	14.7	4,689	19.2
Telecoms	665	-1.0	659	-1.0
Internal services	2,571	0.9	2,669	3.8
Devices	685	15.0	651	-5.0
Data centre	408	0.5	425	4.1
Total	**14,266**	**7.6**	**15,528**	**8.8**

INCREASED ADOPTION OF CLOUD STRATEGIES AND CITIZEN DIGITAL IDENTITY

The pandemic has amplified the need for governments to rapidly scale IT infrastructure and application systems and respond to unprecedented public demands. Gartner estimates that by 2025, over 50% of government agencies will have modernised critical core legacy applications to improve resilience and agility.

"Key national technology capabilities, whole-of-government cloud and SaaS procurement agreements, and digital skills have progressed at a federal level within Australia," said Ferreira.

"We have also seen a strengthening digital mandate in ministerial roles with cross federal–state collaboration at a state level."

MELBOURNE
CONVENTION
& EXHIBITION
CENTRE

COMMS CONNECT

Events for critical communications users and industry

MELBOURNE

8-10 MARCH 2022

FREE EXPO ENTRY

EARLY BIRD RATES END 17 DECEMBER. REGISTER NOW!

Featured speakers:

Shane Fitzsimmons AFSM
Commissioner
Resilience NSW

Lynn McDonald
Azure Space Lead
for Australia

Mats Henrikson
Group Leader
CSIRO Data61

Ed Parkinson
CEO
FirstNet USA

Jackie Dujmovic
Founder and CEO
Hover UAV

Neal Richardson
Technical Director
NZ Police
NGCC Lead Agency

What's on:

- Industry-focused case studies and technical presentations
- Panel sessions on public safety, state of the industry and satellite evolution
- Extensive exhibition and networking opportunities
- ARCIA Industry Gala Dinner on 9 March

Half-day workshops – 8 March

- Power supply options for communications systems, including solar and battery options
- Latest initiatives and innovations in critical LMR, critical broadband 4G/5G and control centres
- Private LTE/5G – the fundamentals of technology and system design
- ACCF Public safety communications 'town hall' meeting

BE INVOLVED

Contact Narelle Granger ngranger@wfmedia.com.au for sponsorship and exhibition enquiries

Platinum Sponsors: hypha by Wireless Innovation; Hytera Respond & Achieve; simoco wireless solutions

Gold Sponsors: ZETRON; powerbox; BENELEC; L3HARRIS FAST. FORWARD.; GME; DAMM; ROHDE&SCHWARZ; BT

Silver Sponsors: CN challenge networks; NEC; Private LTE; SITE PRO 1 A valmont COMPANY; Ace

Media Partner: comms critical

Association Partners: ARCIA; TCCA

Visit www.melbourne.comms-connect.com.au for more information

HOW AI IS TRANSFORMING CUSTOMER EXPERIENCE

©stock.adobe.com/au/fizkes

The impacts of artificial intelligence (AI) in today's businesses can be far-reaching. Organisations can leverage AI tools and solutions to achieve benefits such as more streamlined communications through automation or digitisation that help to achieve greater process efficiencies. However, one of the biggest impacts of AI is on the human side of the equation, especially when it comes to its uses in contact centres, according to software solutions provider NICE.

Rod Lester, Managing Director ANZ, NICE, said these tools are there to support agents, rather than replace them.

"AI can have major impacts and benefits for the human contact centre workforce. While previously contact centre agents may have been concerned that AI would replace the human element, businesses can achieve more benefits by leveraging AI to support human agents rather than replace them. Using AI can enhance both the agent and customer experience (CX) in contact centres," he said.

On average, contact centre agents spend 14% of their working time looking for information required to do their jobs. In an average eight-hour workday, this equates to more than an hour a day of productivity costs due to inefficient processes. However, AI tools like virtual assistants, automation and machine learning can improve efficiencies across the board.

"Contact centres that leverage AI solutions — especially technologies like virtual assistants, augmented intelligence and automation — can essentially provide immediate access for human agents to more specific and useful information about caller behaviours and interactions. Virtual assistants combined with automation especially can help agents access the information they need immediately, rather than investing 14% of their time manually retrieving it," Lester said.

By improving the agent experience and empowering agents to streamline efficiencies and productivity across the board, AI technologies will also improve the customer experience. AI technologies can facilitate better training for contact centre agents and, when combined with machine learning, can be optimised to analyse caller interactions and provide real-time guidance for agents by using qualitative metrics such as call sentiment or behaviours.

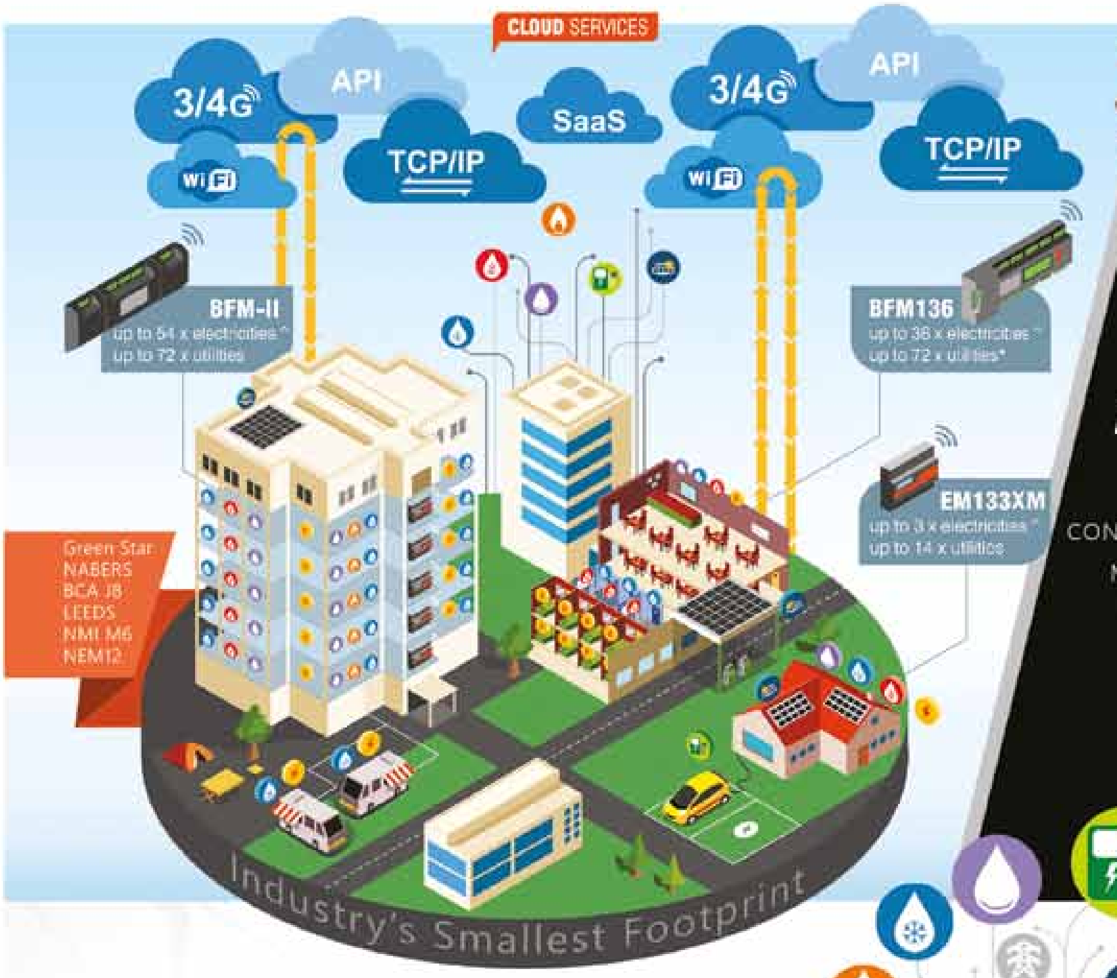
"When agents have access to the information they need at their fingertips, they can provide quicker and more efficient experiences to customers during interactions. Similarly, by leveraging real-time guidance and immediate feedback to agents through the analysis of call interactions, agents can learn faster and reduce errors, leading to more positive CX," Lester said.

In addition to improving CX on calls with human agents, AI technologies can also be used across omnichannel environments. Machine learning can help uncover trends in customer data and behaviours, which can lead to more comprehensive insights into customer churn and repeat contact, for example.

"AI can be an exceptionally useful tool for improving CX, both in terms of the way human agents interact with customers and in the channels that customers use to engage with contact centres. By leveraging AI tools and technologies as part of digital transformation, organisations can achieve significant improvements to operations and efficiencies," said Lester.

SATEC
Powerful Solutions

T +61 2 4774 2959
sales@satec-global.com.au
www.satec-global.com.au



SCALABLE METERING ARCHITECTURE BY SATEC

CONFORMS TO NER CHAPTER 7

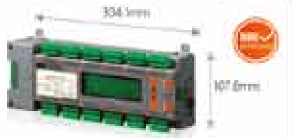
MIXED USE DEVELOPMENTS
URBAN RE-DEVELOPMENT
HYPER-DENSE METERING
SOLAR-PV MULTI ARRAY
VEHICLE CHARGING
SHOPPING CENTRES
STREET LIGHTING
CARAVAN PARKS
GRANNY FLATS
APARTMENTS

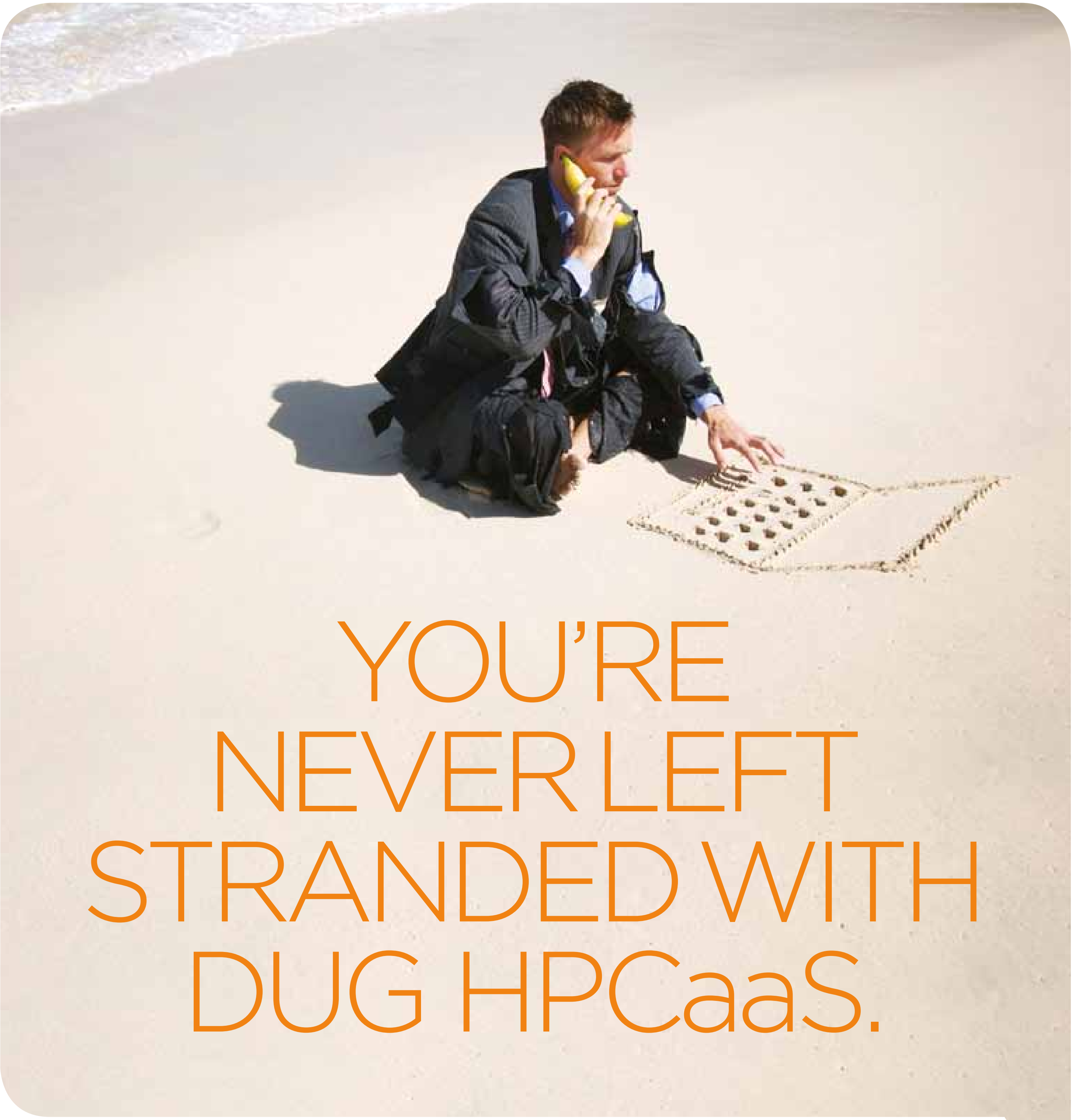
POWER OF CHOICE COMPLIANT SOLUTIONS

> Accuracy Class 0.5S per IEC/AS 62053-22
> 5-Minute Market Settlement Data Ready
> MV90xi - Ethernet, WiFi, 4G, RS485
> Dual communication options
> Remote Disconnect Relay
> RESTful API (JSON) - SaaS

Take control of your utilities from any device anywhere

SCALABLE ARCHITECTURE

NMI APPROVED	 125mm 90mm Power of Choice Ready	 304.1mm 107.6mm	 278mm 128mm
MODEL	EM133XM	BFM136	BFM-II
INSTALLATION TYPE	SMALL	MEDIUM	LARGE
*ELECTRICITIES Tenants	Up to 3	Up to 36	Up to 54
UTILITIES Water, Gas	Up to 14	*Up to 72 With BFM utility module	Up to 72


YOU'RE NEVER LEFT STRANDED WITH DUG HPCaaS.